

مجموعه کتابهای ۱۰۰ گام جادویی

آموزش گام به گام

مقابله و شکست ویروس‌های کامپیوتری

Warning

Virus alert!

OK

به همراه CD
رایگان برنامه‌های
سودمند اینترنت

مؤلف:
ابوالفضل طاهریان ریزی

«بسمه‌تعالی»

آموزش گام به گام

مقابله و شکست ویروس‌های کامپیوتری

مؤلف:
ابوالفضل طاهریان ریزی



انتشارات طاهریان

سرشناسه: طاهریان ریزی، ابوالفضل، ۱۳۵۲ -
عنوان و نام پدیدآور: آموزش گام به گام مقابله و شکست ویروس‌های کامپیوتری/مولف ابوالفضل طاهریان ریزی.
مشخصات نشر: تهران: طاهریان، ۱۳۹۰.
مشخصات ظاهری: ۱۶۸ ص: مصور، جدول، نمودار.
شابک: ۵-۷۹-۸۴۰۶-۹۶۴-۹۷۸
وضعیت فهرست نویسی: فیپا
موضوع: ویروس‌های کامپیوتر
موضوع: اشکال زادی (کامپیوتر)
رده بندی کنگره: ۱۳۸۹ ۱۸ط۹و/QA۷۶
رده بندی دیویی: ۰۰۵/۸۴
شماره کارشناسی ملی: ۲۲۴۲۷۸۱



« آموزش گام به گام مقابله و شکست ویروس‌های کامپیوتری »

● **مؤلف:** ابوالفضل طاهریان ریزی
● **ناشر:** انتشارات طاهریان ● **نوبت چاپ:** اول ● **سال چاپ:** ۱۳۹۰ ● **تیراژ:** ۵۱۰۰ جلد
● **لیتوگرافی:** باران ● **قیمت:** ۶۰۰۰۰ ریال ● **طرح جلد:** آرزو خسروپور
شابک: ۵-۷۹-۸۴۰۶-۹۶۴-۹۷۸

آدرس: میدان انقلاب، خیابان کارگر جنوبی، خیابان لبافی نژاد، پلاک ۲۶۶، طبقهٔ چهارم، واحد ۱۱
تلفن: ۶۶۴۹۲۷۳۳ تلفکس: ۶۶۹۷۴۱۵۲

سفارش مستقیم از طریق وب سایت ما **www.Taherianpress.com**

تقدیم به هنرمند مردمی ایران

مرحوم فرهاد مهرداد

یادش گرامی باد

مقدمه:

با گسترش استفاده از کامپیوتر در تمامی جوانب زندگی انسان قرن ۲۱، حالا با دغدغه‌های جدیدی به نام ویروس‌های کامپیوتری و هکرها روبرو هستند. همانطور که در دنیای واقعی هیچ‌کس نیست که بتواند ادعا کند تا به حال اصلاً به ویروس سرماخوردگی دچار نشده در دنیای کامپیوترها نیز ویروسی شدن امری غیرقابل اجتناب است.

سرعت انتشار ویروس‌ها و میزان خسارت آنها باعث شده که هر سازمان، مدیر و کاربر حرفه‌ای کامپیوتر لازم است توجه ویژه‌ای به آن داشته باشد. در تأیید این ادعا همین بس که ویروس MY Doom در عرض مدت کوتاهی توانست میلیون‌ها کامپیوتر را در سراسر دنیا آلوده کند، سرعت انتشار و گسترش این ویروس و میزان تخریب آن به حدی بود که بیل‌گیتس رهبر مایکروسافت برای دستگیری و معرفی نویسندهٔ این ویروس ۲۵۰ هزار دلار تعیین کرد.

ولی واقعاً ویروس‌های کامپیوتری چه هستند؟ چگونه عمل می‌کنند؟ آیا ویروس‌ها انواع و اقسامی دارند؟ چگونه می‌توان از رسوخ ویروس‌ها به کامپیوترها جلوگیری کرد؟ هکرها چه هستند؟ چگونه می‌توان یک گارد محافظتی را در کامپیوتر خود ایجاد کنیم و ...

پاسخگویی به تمام این سئوالات انگیزه‌ای شد تا من کتابی را در این موضوع تدوین کنم و کتابی که در دست دارید حاصل این تلاش است.

پیش‌فرض

در این کتاب فرض بر آن گذاشته شده که شما با سیستم عامل ویندوز XP (یا ویندوز ۷) و اینترنت آشنا هستید. در صورت عدم این توانایی شما می‌توانید از کتاب‌های آموزش گام به گام ویندوز ۷، کتاب آموزش گام به گام کامپیوتر و ویندوز XP و آموزش گام به گام اینترنت بهره ببرید.

خدمات جانبی کتاب

شما با مطالعهٔ این کتاب به یکی از اعضای خانوادهٔ بزرگ انتشارات طاهریان مبدل شده‌اید ما ورود شما را تبریک گفته و به اطلاع می‌رسانیم که این مؤسسهٔ انتشاراتی امکانات ویژه‌ای را به شرح زیر در اختیار شما قرار می‌دهد:

۱- **پشتیبانی اطلاعات:** این مؤسسهٔ انتشاراتی آمادگی دارد به تمامی سئوالات ریز و درشت خوانندگان کتاب در مورد ویروس‌ها در حد توان پاسخ گفته و راهنمایی‌های لازم را به صورت کاملاً رایگان ارایه دهد. برای این منظور با شماره پشتیبانی ۶۶۹۷۴۱۵۲ تماس بگیرید و سئوالات خود را با کارشناس مربوطه مطرح فرمایید. ما به عنوان یک دوست همیشگی در کنار شما هستیم.

۲- **امکانات جانبی:** همراه با این کتاب یک DVD رایگان که حاوی برنامه‌های سودمند کامپیوتر است، بنابر این هنگام خرید کتاب از وجود این DVD مطمئن شوید.

۳- **وب سایت:** انتشارات طاهریان با ایجاد وب سایت خود به آدرس www.Taherianpress.com سعی کرده یک گام دیگر به شما نزدیک شود. با ورود به این وب سایت شما می‌توانید به آخرین خبرها و اطلاعات در مورد ویروس‌ها و برنامه‌های کامپیوتری دست پیدا کنید. علاوه بر این، ما لیستی از جدیدترین کتاب‌های خود را در آن قرار داده‌ایم که شما با کلیک بر روی آنها می‌توانید خلاصه‌ای از کتاب را نیز مطالعه کرده و آنها را خریداری کنید.

و اما یک خواهش

در این کتاب سعی شده اطلاعات کاملی در مورد ویروس‌ها، هکرها و نحوهٔ مقابله به آن ارایه شود. ما مطمئن هستیم که شما با مطالعهٔ دقیق آن می‌توانید با این پدیده‌های شوم مقابله کنید. پس اولاً با استفاده از E-mail ما را از پیشرفت‌های مداوم خود مطلع کنید و دوماً در صورتیکه از این کتاب راضی بودید آنرا به دیگر دوستانتان نیز معرفی کنید و بدانید که این ایده‌آل‌ترین راه برای کمک به ما است. راستی آدرس E-mail ما Taherian52@gmail.com است.

کلام آخر

شادترین لحظات، پربارترین اوقات و کارآمدترین تجربیات را در هنگام مقابله با ویروس‌ها و هکرها در دنیای کامپیوتر و اینترنت برای شما آرزومندیم.

همیشه پویا باشید

فصل اول: ویروس‌های کامپیوتری

فصل ۲: آیا کامپیوتر من ویروسی است؟

فصل ۳: هکرها

فصل ۴: برنامهٔ ضدویروس

فصل ۵: نصب و نگهداری برنامهٔ ضدویروس

فصل ۶: مقابله با ویروس‌ها

فصل ۷: انتخاب بهترین برنامهٔ ضدویروس

فصل ۸: معرفی ده برنامهٔ ضدویروس مهم

فصل ۹: داستان‌هایی در مورد ویروس‌ها

فصل ۱۰: معرفی برنامهٔ ضدویروس Norton

فصل ۱۱: برنامهٔ ضدویروس McAfee

فصل ۱۲: معرفی خطرناک‌ترین ویروس‌های دنیا

فصل ۱

ویروس‌های کامپیوتری

آیا شما تا به حال در مورد ویروس های بیماری زا چیزی شنیده اید؟ ویروس های بیماری زا (مثل آنفولانزا) پس از ورود به بدن شروع به تکثیر کرده و در صورت عدم توجه به مراقبت های لازم، سیستم دفاعی بدن را از کار می اندازند.

ویروس های کامپیوتری تا حد زیادی به ویروس های بیماری زا شباهت دارند. ویروس های کامپیوتری در حقیقت **برنامه های کوچکی** هستند که با وارد شدن به کامپیوتر آن را آلوده می کنند.

ویروس های کامپیوتری مصداق دقیق ضرب المثل فلفل نبین چه ریزه است حجم یک ویروس می تواند تنها ۹۰ بایت باشد که حتی از حجم سطرهای این صفحه نیز کمتر است. برای روشن شدن و درک خطر ویروس ها بهتر است مثالی بزنیم. فرض کنید شما آشپز بزرگ یک رستوران مجلل هستید که بر اساس دستورالعمل هایی مکتوب قدیمی اقدام به درست کردن یک سوپ خوشمزه می کنید. حال تصور کنید فردی با نیتی خرابکارانه دستورالعملی مثل اضافه کردن یک لیوان فلفل قرمز را به دستوالعمل پخت سوپ شما اضافه کند و شما با پیروی از دستوالعمل فوق (طبق عادت همیشگی) سوپی را برای مشتریان درست کنید. نتیجهٔ نهایی بسیار وحشتناک می باشد خودتان تصور کنید.

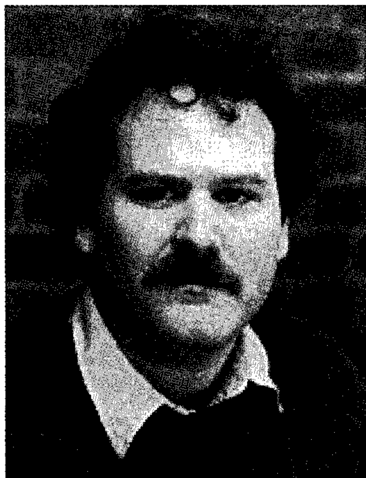


گام اول: تاریخچهٔ به وجود آمدن ویروس‌ها

راستی ویروس های کامپیوتری از کجا آغاز به کار کردند؟ و آیا ویروس های کامپیوتری از همان ابتدا به این خطرناکی بودند؟ این پرسش هایی است که بارها در ذهن ما و شما ایجاد شده است و مطمئناً برای هر یک از آنها پاسخ هایی را در نظر گرفته ایم.

در این گام ما قصد داریم با نگاهی پرسش گرانه، جواب های قانع کننده ای را برای این سئوالات و پرسش ها پیدا کنیم.

پدر واقعی ویروس های کامپیوتری

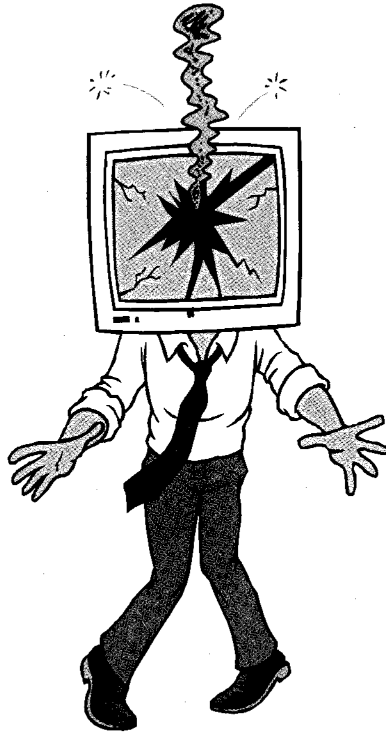


تاریخچهٔ به وجود آمدن ویروس های کامپیوتری به حدود ۳ دههٔ پیش باز می گردد. هنگامی که دانشجویی به نام «**فرد کوهن**» در دانشگاه کالیفرنیای جنوبی به عنوان رسالهٔ دکترای خود در رشتهٔ مهندسی برق، تحقیقات خود را بر روی برنامه ای ارایه کرد که قادر بود یک کپی از خودش را با دستکاری کردن برنامه های دیگر، درون آنها قرار دهد. موضوع رسالهٔ دکترای وی با واکنش های متفاوتی روبرو گردید. ولی این واقعیتی است که حتی خود کوهن نیز تصور نمی کرد که روزی طرح وی به صورت یک فاجعهٔ جهانی در دنیای کامپیوتر تبدیل شود.

> ☺ **همراه:** بله این واقعیتی است که اولین ویروس به وسیلهٔ برنامه نویسان جهت **نمایش خلاقیت** خود ابداع گردید.

اولین ویروس های کامپیوتری

بر اساس مدارک موجود اولین ویروس کامپیوتری به معنای توسط **بسیط فروغ علوی** و **امجد فروغ علوی** صاحبان شرکت کامپیوتری Brain در سال ۱۹۸۵ به نام Brain نوشته شد. این دو برادر پاکستانی با تولید و نگارش برنامه های نرم افزاری در شرکت کامپیوتری خود تجارت می کردند. آنها پس از مدتی متوجه گردیدند که از برنامه های نرم افزاری آنها کپی های غیر مجاز زیادی گرفته می شود.



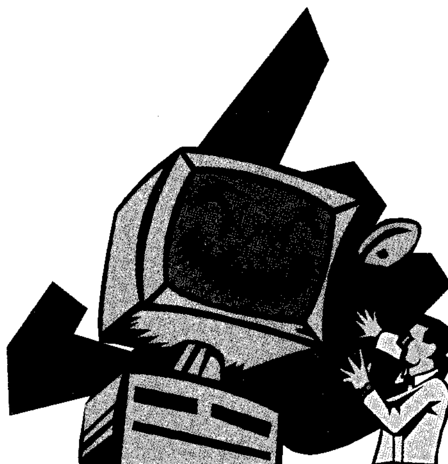
این دو برادر پی برده بودند که هر فلاپی دیسک، حاوی سکتور راه اندازی است که با هر بار راه اندازی سیستم اجرا می گردد. در نتیجه تصمیم گرفتند که برنامه ای را بنویسند که جایگزین این سکتور راه انداز شود به نحوی که اگر کسی خواست از نرم افزار کپی بگیرد سیستم کامپیوتری وی دچار مشکل گردد.

کامپیوتر فرد خاطی به محض تهیهٔ کپی دچار مشکل می شد و پیغامی به این مضمون در روی صفحهٔ نمایش ظاهر می شد که «**به سیاه چال خوش آمدید!**».

استفاده کننده در این حالت هیچ چاره ای جز تماس با برادران علوی جهت ویروس یابی نداشت. البته شماره تلفن برادران علوی بصورت یک پیغام ارایه می شد. این دو برادر با فروش کپی نرم افزارهای معروف دنیا مثل لوتوس و word star با قیمتهای بسیار ارزان، به همهٔ مردم علی الخصوص توریست های خارجی، اقدام به انتشار این برنامه که بعد به **ویروس** شهرت یافت کردند. به زودی این ویروس توانست **صد هزار کامپیوتر** را به راحتی آلوده کند.

یکی از اولین ویروس هایی که نسبت به ویروس Brain بسیار مخرب تر می باشد ویروس اُرشلیم می باشد. این ویروس اولین بار در سال ۱۹۸۷ در دانشگاه عبری فلسطین اشغالی گزارش شده و اصلیت آن اسرائیلی می باشد.

این ویروس در روز جمعه سیزدهم ماه می ۱۹۸۸ (یعنی چهلمین سالگرد ایجاد دولت غاصب اسرائیل) فعالیت تخریبی خود را آغاز کرده و پس از پاک کردن تمام فایل های کامپیوتری به کار خود خاتمه می داد.



ویروس اُرشلیم به صورتی برنامه نویسی شده تا در جمعه یا ۱۳ هر ماه از خود کپی هایی را تهیه کرده و به برنامه های دیگر بچسباند. این ویروس کامپیوترهای بسیاری از دانشگاه ها و مراکز نظامی را آلوده و تخریب کرد.

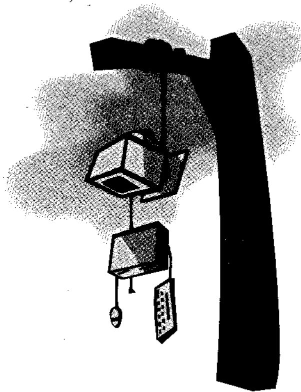
☺ بیشتر بدانیم! آیا برای شما تعجب آور نیست که **ویروس خطرناک ساسر** که کمتر از یک هفته ۱۸ میلیون کامپیوتر را در سراسر دنیا آلوده کرد و موجب تعطیلی موقت چند شرکت بزرگ کامپیوتری شد به وسیلهٔ یک **جوان ۱۸ساله** به نام **Sven Jaschan** نوشته شده است. گفتنی است که شرکت بزرگ مایکروسافت برای دستگیری نویسندهٔ نابغهٔ این ویروس مبلغ ۲۵۰ هزار دلار جایزه تعیین کرده بود. این جوان بالاخره پس از حملهٔ ناگهانی پلیس به منزل وی در شهر روتنبرگ آلمان دستگیر شد.

خطر ویروس های کامپیوتری در دنیای امروزی با گسترش کامپیوتر در کلیهٔ جوانب زندگی ما پر رنگ و پر رنگ تر شده است.

گام دوم: ساختار کلی ویروس‌ها

اکثر کاربراین کامپیوتر، ویروس ها را برنامه های هوشمند و کاملاً خطرناک می دانند که خود به خود تکثیر و اجرا شده و اثرات مخرب فراوانی دارند که باعث از بین رفتن اطلاعات و گاه خراب شدن کامپیوتر می گردند.

در حالیکه طبق آمار منتشر شده تنها ۵ درصد از ویروس ها دارای اثر تخریبی بوده و بقیهٔ صرفاً تکثیر می شوند. بنابر این یک ویروس را می توان برنامه ای دانست که می تواند با استفاده از یک میزبان شروع به تکثیر نماید.



ویروس های کامپیوتری برنامه هایی هستند که به وسیلهٔ ویروس نویسان نوشته شده و سپس به طور ناگهانی توسط یک فایل اجرایی و یا جای گرفتن در ناحیهٔ سیستمی دیسک، فایل ها و یا کامپیوترهای دیگر را آلوده می کنند.

عملکرد یک ویروس را می توان به صورت خلاصه به چهار بخش ساده تقسیم کرد:

- ✓ **ورود ویروس به کامپیوتر میزبان**
- ✓ **تکثیر ویروس**
- ✓ **تخریب اطلاعات**
- ✓ **الحاق به برنامه های دیگر و نفوذ به کامپیوترهای دیگر**

لذا یک ویروس می تواند پس از اندک زمانی در کامپیوترهای موجود یک کشور و یا حتی در سراسر دنیا منتشر شود. از آنجا که ویروس ها به طور مخفیانه عمل می کنند، تا زمانیکه کشف نشده و امکان پاکسازی آنها فراهم نگردیده باشد، برنامه های بسیاری را آلوده می کنند.



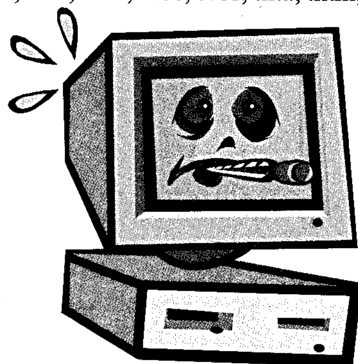
میزبان ویروس ها

ویروس نیز همانند هر برنامهٔ کامپیوتری دیگر نیاز به محلی جهت ذخیره سازی دارد. منتهی این محل باید به گونه ای باشد که ویروس ها را به اهداف خود نزدیک و نزدیکتر کند.

اصولاً فایل های موجود در یک کامپیوتر را می توان به دو گونهٔ فایل های «**اجرایی**» و «**غیر اجرایی**» تقسیم کرد. هدف اصلی اکثر ویروس ها، فایل های اجرایی و آلوده کردن آنها می باشند و کمتر ویروسی را می توان یافت که در یک فایل غیر اجرایی قرار گرفته و از طریق آن تکثیر شود.

در فهرست ذیل پسوند فایل های اجرایی رایج کامپیوتر گرد آمده است:

.com, .exe, .dll, .ovl, .bin, .sys, .dot, .doc, .vbe, .vbs, .hta, .htm, .scr, .ocx, .hlp, .eml



☺ همراه: لازم به ذکر است که بعضی از فایل ها را شاید نتوان ذاتاً اجرایی دانست ولی چون اینگونه فایل ها می توانند حاوی **قسمتهای اجرایی** باشند لذا آنها را از نوع اجرایی در نظر می گیریم. از این نوع فایل ها می توان به فایل های **Html** و مستندات برنامه های **Office** اشاره کرد که به ترتیب ممکن است شامل

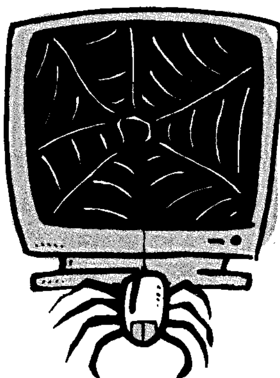
اسکریپت و ماکرو باشند. اسکریپت ها و ماکروها قسمتهای اجرایی هستند که در دل این فایل ها قرار گرفته و عملکرد خاصی را انجام می دهند.

بعضی از ویروس ها علاوه بر تأثیر گذاری بر روی فایل های اجرایی، قابلیت استفاده از سکتور راه انداز (Boot Sector) و جدول پارتیشن بندی دیسک (Partition Table) به عنوان میزبان را دارا می‌باشند.

سکتور راه انداز، **واحد راه اندازی** سیستم عامل است که در سکتور شمارهٔ صفر فلاپی دیسک و یا درایوهای منطقی یک هارد دیسک قرار دارد.



جدول پارتیشن بندی شامل اطلاعات **تقسیم بندی هارد دیسک** می باشد که آن نیز در سکتور شمارهٔ صفر هارد دیسک قرار دارد. اینگونه ویروس ها با قرار گرفتن در یکی از این دو محل، هنگام راه اندازی کامپیوتر، اجرا شده و در حافظهٔ سیستم مقیم می شوند و تا زمان خاموش کردن کامپیوتر یا راه اندازی دوباره، همانجا مانده و فلاپی ها یا هارد دیسک های دیگر را آلوده می کنند.



ویروس های بی خطر

همانطور که اشاره شده تنها پنج درصد از ویروس های کامپیوتری دارای اثرات تخریبی هستند و بقیه صرفاً تکثیر می شوند. حالا سئوال این است که آیا این ویروس های **به اصطلاح بی خطر** هیچ تأثیر منفی بر عملکرد کامپیوتر ندارند؟ جواب به این پرسش را می توان در چندین قسمت پاسخ گفت:



• بسیاری از ویروس های بی خطر دارای اثراتی هستند که برای کاربر **ایجاد مزاحمت** می کنند. مثلاً ممکن است پیغامی را نمایش دهند که باعث ریزش حروف صفحهٔ نمایش به پایین شوند و یا اینکه یک آهنگ پخش کنند.

علاوه بر این برخی از ویروس ها به علت اشکالات نرم افزاری که ناشی از عدم دقت ویروس نویس می باشد، ممکن است دارای اثرات غیر قابل پیش بینی باشند، که در بعضی مواقع حتی می توانند تخریبی باشند.

• برخی از این ویروس های بی خطر در حافظهٔ کامپیوتر شما مقیم شده و از این طریق عملیات تکثیر خود را انجام می دهند. این عمل ممکن است به گونه ای باشد که فضایی برای اجرای برنامه های دیگر نماند و یا باعث **ایجاد تأخیر** و **وقفه** در حین عملیات سیستم، اعم از اجرای برنامه ها و یا راه اندازی، کامپیوتر گردند.

• ویروس های زیادی هستند که عملکرد تخریبی ندارند ولی کارهای دیگری مثل **سرقت اطلاعات** و **کلمهٔعبور کاربر** را انجام می دهند. بعضی از اینگونه برنامه ها با مقیم شدن در حافظه از عباراتی که توسط شما تایپ می شود گزارش گرفته و پس از اتصال کامپیوتر شما به اینترنت، این اطلاعات را برای مقصد خاصی ارسال می کنند. گیرندهٔ این اطلاعات می تواند به راحتی از این اطلاعات سوء استفاده های مختلفی را بکند.

• یک ویروس علی رغم بی خطر بودن با انتقال غیر عمدی می تواند باعث عدم اعتماد افراد به یکدیگر شود.

☺ همراه: این نکته را مد نظر داشته باشید که یک ویروس در خوشبینانه ترین حالت، وقت ریزپردازنده و فضای هارد دیسک شما را تلف می کند.

بیشتر بدانیم: کتابی به نام ویروس‌ارسطو
یکی از مجرمین اصلی ویروس نویسی به نام مستعار «**ارسطو**» می گوید: «نگارش یک ویروس غیر قانونی نیست و باید به آن به چشم فرایند خلاق **مثل نوشتن یک کتاب** نگاه شود. امروزه برخی از افراد کتابهای جنایی می نویسند که خیلی خرابکارانه تر و مضرتر از نوشتن یک ویروس است. پس نباید ویروس نویسی را امری غیر قانونی دانست بلکه باید انتشار آن را جرم دانستن.»

گام سوم: تقسیم‌بندی ویروس‌ها بر اساس آلوده‌سازی

ارائهٔ یک تقسیم بندی دقیق از ویروس ها امری مشکل به نظر می رسد و می توان ویروس ها را به روش های مختلفی تقسیم کرد. این روش ها می تواند بر اساس نوع میزبان ویروس، سیستم عاملی که ویروس می تواند در آن فعالیت کند، روش آلوده سازی فایل و ... باشد. در زیر به برخی از این روشهای آلوده سازی اشاره می کنیم:

☜ **ویروس های فایلی (File Viruses)**

این ویروس ها (همانطور که قبلاً به آن اشاره کردیم) معمولاً فایل **های اجرایی** را آلوده می کنند. فایل های آلوده به این نوع ویروس اغلب دارای پسوند com. یا exe. می باشند.



☜ ویروس های ماکرو (Macro Viruses)

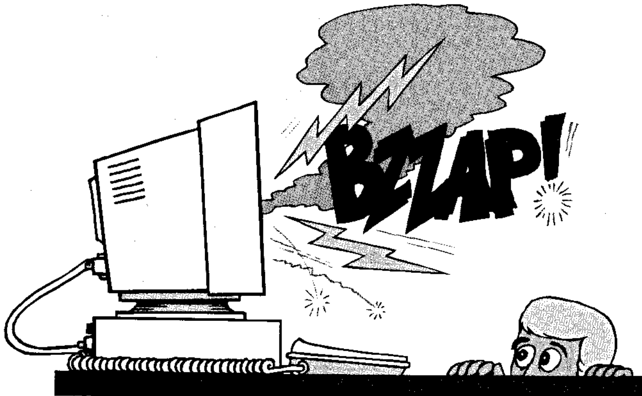
ویروس های ماکرو، مستندات برنامه هایی را که از **امکان ماکرونویسی** پشتیبانی می کنند (مانند Ms Excel, Ms Word و ...) آلوده می کنند.
فایل های اینگونه برنامه ها اجرایی نیستند ولی درون آنها قسمتهای اجرایی به نام «ماکرو» وجود دارد که می تواند میزبان مناسبی برای ویروس های کامپیوتری ماکرو باشند.



☜ ویروس های بوت و سکتور و جدول پارتیشن بندی (Boot Sector and Partition Table Viruses)

اینگونه ویروس ها سکتور راه انداز (Boot Sector) هارد دیسک و فلاپی دیسک یا **جدول پارتیشن بندی هارد دیسک** را آلوده می کنند. با راه اندازی سیستم از روی دیسکی که به این ویروس ها

آلوده اند، ویروس در حافظه مقیم شده و متعاقباً دیسکهایی را که مـورد دسترسـی قـرار مـی‌گیرنـد، آلوده می شود.



ویروس های اسکریپتی (Script Viruses)

این ویروس ها اسکریپت های نوشته شده به زبان های برنامه نویسی ویژوال بیـسیک یـا جـاوا مـی باشند و تنها در کامپیوترهایی اجرا می شوند که بـر روی آنهـا مرورگـر Internet Explorer یـا هـر مرورگر وب دیگری با **توانایی اجرایی اسکریپت ها**، نصب شده باشد. این ویروس سپس بـه آلـوده سازی فایل هایی با پسوند .html, .htm, .vbs, .js, .htt یا .asp می پردازند.

گام چهارم: تقسیم‌بندی فرعی ویروس‌ها

علاوه بر تقسیم بندی ویروس ها بر اساس مقصد آلوده سازی می توان کلیهٔ ویروس های موجود را در یکی از تقسیم بندی های زیر قرار داد:

ویروس های مقیم در حافظه (Memory Resident Viruses)

اینگونه ویروس ها با مقیم شدن در حافظه، هنگام دسترسی به فایل های دیگر، آنها را آلوده می کنند.

ویروس های مخفی کار (Stealth Viruses)

اینگونه ویروس ها به روش های مختلف ردپای خویش را **مخفی** می کنند. به این معنی که فایـل هـای آلوده به اینگونه ویروس ها به گونه ای نشان داده می شوند که بصورت یک **فایل غیر آلـوده جلـوه** می کنند. به عنوان مثال عموم ویروس ها پس از آلوده کردن یک فایل، اندازهٔ آن را افزایش می دهنـد و یا گاهی تاریخ و زمان ثبت فایل را عوض می کنند. امـا ویـروس هـای مخفـی کـار، مـی تواننـد بـا روش‌هایی خاص و بدون تغییر ظاهری، عملیات خویش را انجام دهند.



ویروس های کد شده (Encrypting Viruses)

این ویروس ها پس از هر بار آلوده سازی، با استفاده از شیوه های خود رمزی، شکل ظاهری خود را تغییر می دهند.

ویروس های چند شکله (Polymorphic Viruses)

اینگونه ویروس ها با استفاده از الگوریتم های خاص، علاوه بر تغییر شکل ظاهری خود، **ساختار خود را نیز تغییر** می دهند به طوریکه ممکن است جای دستورالعمل ها و حتی خود دستور العمل ها نیز تغییر کنند.

ویروس های فعال شونده بر اساس رویدادی خاص (Triggered Event Viruses)

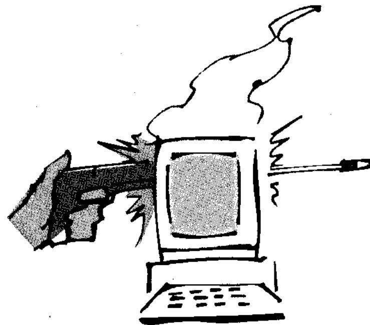
ویروس هایی هستند که بخشی از عملیات تخریب خود را در ساعت یا **تاریخی خاص** انجام می دهند. البته باید توجه داشت که تکثیر و آلوده سازی فایلها در زمان فعال بودن ویروس انجام می شود. ویروس ارشلیم از این نوع ویروس ها می باشد.

گام پنجم: برنامه‌های مخرب موسوم به ویروس

به غیر از ویروس ها، برنامه های خطرناک دیگری نیز وجود دارند که به علت مخرب بودن و جستجو و شناسایی شدن توسط برنامه های ضد ویروس به ویروس مشهور هستند. البته واقعیت این است که این برنامه ها به دلیل عدم توانایی در تکثیر از طریق یک میزبان با ویروس های کامپیوتری تفاوت دارند. ولی می توان آنها را در زمرهٔ ویروس های کامپیوتری طبقه بندی کرد:

کرم *(Worm)*

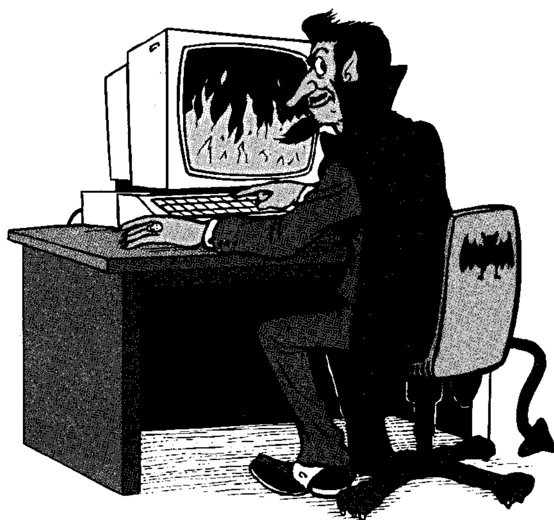
کرم کامپیوتری برنامه ای مخرب است که قسمت های استفاده نشدهٔ **حافظهٔ** اصلی کامپیوتر را جستجو کرده و سپس خود را در آن محل آنقدر **تکثیر** می کند تا کل قسمت خالی حافظه را اشغال کرده و بالاخره تمام حافظه را **فلج** کند، به صورتیکه دیگر کامپیوتر قادر به کار نباشد.
به طور معمول کرم ها برای حرکت و سفر بین کامپیوترها طراحی شده اند و گاهی نیز در محل ورودی یک سیستم به شبکه، قرار گرفته و علاوه بر رمز عبور، **نقاط ضعف سیستم** را ارزیابی می‌کنند. با این حال هدف اصلی کرم ها تکثیر خود می باشد.
این برنامه ها امروزه بیشترین میزان آلوده سازی را به خود اختصاص داده اند. و تنها در یک چشم بر هم زدن این هدف را اجرا می کنند. کرم ها معمولاً از طریق پیوستن به **نامه های الکترونیکی** و حفره های امنیتی در سیستم عامل ویندوز مثل حفرهٔ موجود در RPC و ... منتشر می شوند.



اسب ترویا *(Trojan Horse)*

آیا شما داستان اسبی چون تروی (یکی از افسانه های ایلیاد) را خوانده اید. در این داستان مهاجمان به فرماندهی آشیل برای ورود به شهر تروی از یک اسب چوبی استفاده کرده و با مخفی شدن در داخل آن به شهر نفوذ کرده و آنرا تصرف کردند.
اسب ترویا، برنامه ای ظاهراً بی خطر و مجازی می باشد که در درون خود به صورت مخفی اقدام به عملیات تخریبی می کند. بعضی از نویسندگان با هوش ویروس، این برنامه های مخرب را به صورت **پیوست** یک برنامهٔ رایگان و با ارزش نرم افزاری، توسط E-mail برای دیگران ارسال می کنند.
گیرندهٔ ایمیل از همه جا بی‌خبر به محض نصب این برنامه ها در کامپیوتر خود، آلوده می‌شود.

جالب اینجاست که ممکن است اسب ترویا همراه با برنامه های رایگان بعد از نصب، مدت ها به صورت کامل وظایف خود را انجام ندهد و هیچ گونه آسیبی به کامپیوتر شما نرساند. اما ناگهان اسب ترویا عمل کرده و عملیات تخریبی خود را شروع می کند.

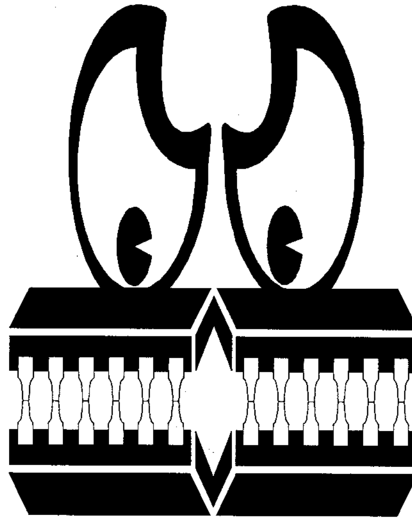


برنامه های جاسوسی (Spyware)

این برنامه ها به صورت مستقیم دارای اثرات تخریبی نمی باشند و وظیفهٔ اصلی آنها **جمع آوری اطلاعات** از روی سیستم کاربر و تحت نظر قرار دادن اعمال کاربر هنگام کار با اینترنت می باشد. اطلاعات مورد نظر این برنامه پیدا کردن شمارهٔ کارت اعتباری، کلمهٔ عبور شبکه، کلمهٔ عبور E-mail (تحت وب) و ... می باشد.

در نهایت این اطلاعات جمع آوری شده طبق تنظیمات تعریف شدهٔ برنامهٔ جاسوسی به مقاصد مورد نظر استفاده می شود.

البته بعضی از **شرکت های تبلیغاتی** و تجاری نیز جهت حصول به اهداف خود، از این برنامه ها استفاده می کنند.



جُک (*Joke*)

همانگونه که از نام این برنامه بر می آید، برنامه های جُک بیشتر جنبهٔ **شوخی** و مزاح دارند. روش کار جُک ها به این صورت است که ادعا می کنند در حال انجام عملیات تخریبی هستند ولی در واقع اینگونه نبوده و کار آنها چیزی جز یک شوخی ساده نمی باشد.

متأسفانه بعضی از کاربران، این برنامه ها را بسیار جدی می گیرند و با تلاش برای از بین بردن چیزی که مخرب نیست **باعث ایجاد** تخریب های بیشتری می شوند.

بمب های ساعتی (*Logic Bomb*)

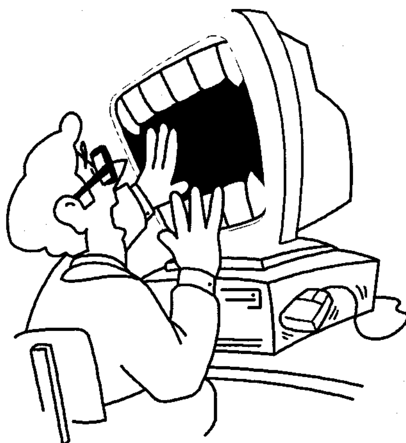


یکی از مخرب ترین گونه های برنامه های مخرب، بمب های ساعتی می‌باشد که شناسایی آن بسیار مشکل است. این برنامه های مخرب عملیات خود را به محض ورود به سیستم شروع نمی کنند، بلکه در گوشه ای در **کمین** می نشینند و در زمان مناسب طبق برنامه ریزی تعیین شده برای آنها، همانند یک بمب ساعتی عمل می کنند و شما را غافلگیر می کنند.

بعضی از این برنامه ها بعد از انفجار به خواب رفته و در کمین بوجود آمدن شرایط مجدد انفجار می مانند. متأسفانه شما هنگامی متوجهٔ این بمب های ساعتی می شوید که کار از کار گذشته است.

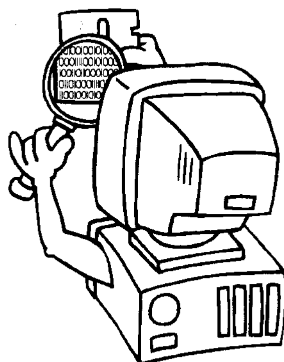
شوخی های غلط انداز *(Hoax)*

این برنامه ها با سوء استفاده از اطلاعات اندک کاربران آنها را فریب داده و با ارایهٔ دستورات و توصیه های اشتباه باعث می شوند که کاربر شخصاً کاری تخریبی را بر روی سیستم خود انجام دهد. به عنوان مثال وانمود می کنند که در مسیر سیستم عامل، فایلی خطرناک وجود دارد و باید به وسیلهٔ کاربر حذف شود. غافل از اینکه این فایل یکی از فایل های مهم سیستمی بوده و ویندوز برای فعال شدن به آن نیاز دارد.



شماره گیرها *(Dialer)*

اینگونه برنامه ها وظیفهٔ اصلی شان ارتباط کاربر از طریق خطوط تلفن به سرورهایی در کشورهای دیگر، جهت دسترسی مستقیم به اطلاعات آنها می باشد. اکثر این برنامه ها بدون اطلاع کاربران عمل کرده و باعث بالا رفتن بسیار زیاد هزینه ها می گردند.



درب مخفی *(Back Door)*

تله ها یا درب های مخفی جزء انواع ویروس ها نمی باشند، بلکه نوعی محل نفوذ و ورود به سیستم‌های کامپیوتری می باشند. سارقان اطلاعات، از این درهای مخفی جهت نفوذ به کامپیوتر و استفاده یا تخریب اطلاعات سیستم بهره می‌برند.

همهٔ تلاش ها برای ورود به یک سیستم کامپیوتری به خارج از آن سیستم محدود نمی شود، بلکه در بعضی مواقع برنامه نویسان و طراحان برنامه، راه هایی را برای نفوذ در درون سیستم امنیتی برای خود قرار می دهند که به درب مخفی معروف است.

به طور مثال از طریق وارد کردن یک رمز عبور سری، وارد کامپیوتر شده و علاوه بر دسترسی به اطلاعات، در بعضی از مواقع به صورت دلخواه آنها را تغییر می دهند. البته بعضی از افراد، ایجاد این درب های مخفی را **حق مسلم خود** می دانند ولی مشکل اینجاست که هکرها نیز از درب های مخفی برای مقاصد خود بهره می برند.



☺ **همراه:** درب های مخفی به **Trap Door** و **Wormholes** نیز معروف هستند.

گام ششم: برنامه‌های جاسوسی SpyWare

در گام قبل ما مختصری در مورد برنامه های جاسوسی صحبت کردیم. به دلیل اهمیت این برنامه ها در این گام قصد داریم نگاه دقیق تری را بر این برنامه که به صورت روز افزونی در حال گسترش هستند داشته باشیم.

همانطور که گفتیم وظیفهٔ اصلی این برنامه ها **جمع آوری اطلاعات** از روی کامپیوتر میزبان و ارسال آنها به مقاصد مختلف می باشد. ولی شاید باور نکنید که یکی از دلایل **کند شدن کامپیوتر** شما همین برنامه های جاسوسی می باشند. این برنامه ها با استفاده از روش های مختلف به کامپیوتر شما وارد شده و مانند یک ویروس، قدرت پردازش کامپیوتر شما را کاهش می دهند.

بعضی از گونه های این برنامه ها با جمع آوری اطلاعات در مورد عادات و کشف علایق شما در اینترنت و ارسال آنها به سایت های ارایه دهنده، با ارایهٔ آگهی های تبلیغاتی و ارسال اسپم ها شما را آزار می دهند.



اسپم ها (Spam) در واقع **نامه های تبلیغاتی ناخواسته ای** هستند که به صورت انبوه برای کاربران اینترنت ارسال می شوند و اغلب به دلیل کثرت، موجبات عصبانیت کاربران را فراهم می کنند.

نحوهٔ ورود برنامهٔ جاسوسی

مجموعهٔ عملکردهای شما در اینترنت باعث نصب برنامه های جاسوسی می شود، مثلاً هنگامی که یک پنجرهٔ شناور را تأیید می کنید و یا بر روی یک اتصال کلیک می نمایید. نصب یک برنامهٔ جاسوسی **بدون هیچ اجازه ای** در روی کامپیوتر شما انجام می گیرد. برنامه های جاسوسی از تکنیکهای مختلفی جهت نصب بهره می گیرند که مهمترین آنهاعبارتند از:

- ☑ **نصب از طریق اینترنت به صورت یک برنامهٔ ضد جاسوسی**
- ☑ **قرار گرفتن به عنوان فایل های پیوستی یک برنامه**
- ☑ **نصب به عنوان مکمل برنامه های مرورگر**
- ☑ **نصب هنگام فعال شدن صفحات وب**



نحوهٔ عملکرد برنامه های جاسوسی

برنامه های جاسوسی با وارد شدن به کامپیوتر شما در قالب یک برنامهٔ کاملاً کاربردی، مقداری از حافظهٔ سیستم و قدرت پردازش کامپیوتر شما را اشغال می کند. مهمترین فعالیت های این میهمانان ناخوانده عبارتند از:

✓ برنامهٔ جاسوسی با رگباری از آگهی های تبلیغاتی شناور، **سرعت مرورگر** شما را تا حد زیادی کاهش می دهند.

✓ برنامهٔ جاسوسی **صفحهٔ خانگی** تنظیمیات مرورگر شما را به صورت دلخواه **تغییر** می دهند.

✓ بعضی از برنامه های جاسوسی مرورگر و **جستجوی شما در اینترنت** را **هدایت** می کنند.

✓ برنامه های جاسوسی **تنظیمات فایروال** شما را **تغییر** می دهند.

✓ برخی از این برنامه ها با **بالا بردن ترافیک تبلیغاتی** در کامپیوتر شما از قبال، این تبلیغات به کسب درآمد می پردازند.

✓ در صورتیکه شما از اینترنت Dial-Up استفاده می کنید بعضی از برنامه های جاسوسی شماره گیری شما را از طریق **شماره تلفن های گرانتر** انجام می دهند.

✓ برخی از این برنامه های جاسوسی به حدی هوشمند هستند که هنگام **حذف** آنها در این کار **اختلال ایجاد** می کنند.

چگونه با برنامه های جاسوسی مقابله کنیم؟

مقابله با برنامه های جاسوسی را شاید بهتر باشد به دو قسمت مجزا تقسیم کرد: **یکی مقابله با برنامه های جاسوسی** که به کامپیوتر شما وارد شده اند و دیگری **مقابله با ورود** برنامه های جاسوسی به کامپیوتر شما. روشهای کارآمد مقابله با برنامه های جاسوسی به شرح زیر است:

- **استفاده و به کارگیری یک برنامهٔ ضد ویروس**: خوشبختانه اکثر برنامه های ضد ویروس دارای یک برنامهٔ ضد جاسوسی نیز می باشند. در ادامهٔ کتاب به معرفی آنها خواهیم پرداخت.
- **از یک برنامهٔ بلوکه کنندهٔ آگهی های تبلیغاتی بهره بگیرید.**
- **تنظیمات Active X مرورگر خود را فعال کنید.**
- **هنگام بستن پنجره های جدید بسیار محتاط باشید.**
- برای بستن پنجره های تبلیغاتی شناور، هنگام مرور صفحات وب بر روی **کلید ضربدر** (☒) پنجره کلیک کنید.

بیشتر بدانیم: ویروسی به نام **Melissa** ۱

یکی ویروس‌های خطرناک، ویروس **Melissa** می باشد. از دلایل سریع انتشار ویروس **Melissa** می توان به تکنیک مؤثر آن در ارتباطات شبکه اشاره کرد. این ویروس پس از **پیدا کردن آدرس های e-mail** دوستان شما در کامپیوترتان، خود را برای تمام کسانی که شما برای آنها شناخته شده می باشید ارسال می کرد و آنها نیز بدون هیچ تردیدی **E-mail** دریافتی را باز و ویروس را دریافت می کردند. این ویروس در سال ۱۹۹۹ به عنوان **سریع ترین ویروس** تا آن تاریخ شناخته شد.

بالاخره در یکم آوریل همان سال **Davie L.Smith** در ایالت نیوجرسی آمریکا به اتهام نوشتن ویروس **Melissa** دستگیر شد.

خلاصهٔ این فصل

خسته نباشید ما در این فصل مطالب زیادی را در مورد ویروس ها و اشکال مختلف آنها فرا گرفتیم که هر کدام قابل تأمل و بررسی بیشتر می باشد. مطالب مطروحه در این فصل را شاید بتوان مهمترین اصل در طرح پروژهٔ دفاعی علیه ویروس ها دانست. امیدواریم نگاه و دیدی روشن از ویروس ها و خطرات آنها پیدا کرده باشید. لطفاً این نکته را همیشه مد نظر داشته باشید که ویروس‌های کامپیوتری همانند ویروس های بیماری زا همه جا هستند شما با حفظ اصول کامل حفاظتی به سادگی می توانید کامپیوتر خود را در مقابل آنها بیمه کنید.

سئوالات تستی

پدر ویروس های کامپیوتری چه کسی است؟

الف: بن لادن　　ب: فرد کوهن

پ: برادران علوی　　ج: دقیقاً مشخص نیست

نام اولین ویروس، نویسندهٔ آن و کشور ارایه دهنده چیست؟

الف: کوهن، فرد، آمریکا

ب: کبیر، جانسون، یونان

پ: Brain، برادران علوی، پاکستان

ج: ارشلیم، دانشگاه عبری، اسرائیل

مراحل چهارگانهٔ عملکرد یک ویروس کامپیوتری را بنویسید؟

الف: ورود، تکثیر، تخریب، نفوذ

ب: ایجاد، تخریب، بازیابی

پ: قالب بندی، از بین بردن اطلاعات، تخریب، مخفی شدن

ج: نفوذ، تخریب، تکثیر، مخفی شدن

فایل های اصلی مورد حمله در اکثر قریب به اتفاق ویروس ها چه فایل هایی هستند؟

الف: فایل های اطلاعاتی

ب: فایل های اجرایی

پ: فایل های پشتیبان

ج: فایل های غیر اجرایی

«سخنان درگوشی»

بعد از مرگ چه اتفاقی برای ایمیل و حساب‌های آنلاین شما رخ می‌دهد؟

راستی چند لحظه‌ای تا به حال فکر کرده‌اید که پس از مرگ ما چه اتفاقی ممکن است برای حساب‌ها، ایمیل و فعالیت‌های آنلاین ما رخ می‌دهد. در انتهای این فصل اتفاق‌هایی که ممکن است برای آنها قابل تصور شود ذکر شده است:

✓ **E-mail**: شرکت Hotmail در کمال امانتداری با دریافت گواهی فوت و اجازه از وکیل شما، یک CD حاوی E-mailهای دریافتی را به خانواده‌تان تحویل می‌دهد. Gmail نیز به همین مدارک نیاز دارد با این تفاوت که شما قبل از مرگ چنین تنظیماتی را در حساب خود ایجاد کرده باشید.

✓ **شبکه‌های اجتماعی**: فیس‌بوک به درخواست خانوادهٔ فرد مرحوم عمل می‌کند. خانوادهٔ شما می‌توانند درخواست حذف حساب‌تان را کرده و یا آنرا به صورت یاد بود حفظ کنند. در این وضعیت امکان به‌روزسازی اطلاعات از بین می‌رود و فقط دوستان می‌توانند در حساب فوق نظر بدهند.

✓ **اشتراک عکس**: سایت فیلکر یکی از بزرگ‌ترین سایت‌های به اشتراک‌گذاری عکس در دنیای آنلاین اکانت کاربران مرحوم خود را همچنان باز نگه می‌دارد. اما در صورتیکه عکسی توسط کاربر قبل از مرگ به صورت خصوصی علامت‌گذاری شده باشد این عکس برای همیشه از دید مراجعه کنندگان پنهان نگه داشته می‌شود. البته بازماندگان می‌توانند این عکس‌ها را از فلیکر تحویل بگیرند.

✓ **رمزهای عبور**: شرکت‌های مختلف ارائه دهندهٔ سیستم‌های مدیریت رمز عبور با دریافت گواهی‌های لازم مبنی بر فوت صاحب حساب، آنها را به وارث تحویل می‌دهند.

فصل ۲

آیا کامپیوتر من ویروسی است؟

عوامل مختلفی می توانند در آلوده شدن کامپیوتر شما به ویروس ها دست داشته باشند. مثلاً شما E-mailهای زیادی را بدون اینکه از آلوده بودن آنها اطلاع داشته باشید دریافت می کنید.
اکثر کامپیوترها در ارتباط با کامپیوترهای آلوده، ویروسی می شوند، بنابراین می توان یکی از دلایل مهم ویروسی شدن یک کامپیوتر را **داشتن همنشین بد دانست**...
در این فصل به اطلاعات جالب و ضروری زیادی جهت پی بردن به ویروسی بودن یا نبودن کامپیوتر خود دست می یابیم. در هنگام بر خورد با انواع و اقسام ویروس ها این مسئله را مد نظر داشته باشید که ویروسی شدن یکی از فرایندهای غیر قابل اجتناب در کار با کامپیوتر و جستجو در اینترنت می باشد. بنابراین هنگام برخورد با این پدیده به **کسب تجربهٔ بیشتر** بیاندیشید.

گام اول: عوامل ویروسی شدن کامپیوترها

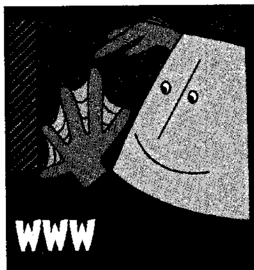
قبل از بررسی و کنکاش کامپیوتر خود در این گام بهتر دیدیم نگاهی به عوامل اساسی در ویروسی شدن کامپیوترها داشته باشیم. نکات و عوامل فهرست شده در این گام در ویروسی شدن قریب به اتفاق کامپیوترها نقش مهم و اساسی دارند.
از عوامل مهم در ویروسی شدن کامپیوتر شما می توان به موارد زیر اشاره کرد:

- ✓ نسخهٔ ویندوزی که شما از آن جهت کار استفاده می کنید.
- ✓ نصب یا عدم نصب برنامه های امنیتی
- ✓ تعداد افرادی که از کامپیوتر شما استفاده می کنند.

عادت های شما در هنگام مرور صفحات وب نیز در ویروسی شدن کامپیوترتان نقش مهم و اساسی دارد. این عادات عبارتند از:

✓ کثرت و تعداد وب سایت های مرور شده توسط کاربر
✓ تغییرات اعمالی از طرف وب سایت های مرور شده
✓ استفاده از پیوست های ارسالی همراه با E-mail
✓ نوع اتصال شما به اینترنت (Dial-Up یا سرویس های پر سرعت)

همهٔ این فاکتورها را می توان در ویروسی شدن کامپیوتر شما مهم و اساسی دانست.



نوع سیستم عامل

همانطور که گفته شد یکی از عوامل مهم ویروسی شدن کامپیوتر را می توان نسخهٔ ویندوزی که شما مورد استفاده قرار می دهید دانست. نسخه های اولیهٔ ویندوز دارای **ویژگی های امنیتی کمتری** نسبت به نسخه های امروزی هستند. بنابراین سعی کنید حدالامکان از نسخه های نهایی ویندوز استفاده کنید.



نحوهٔ اتصال به اینترنت

نحوهٔ اتصال به اینترنت، یکی از فاکتورهای مهم در ویروسی شدن کامپیوترها می باشد. نوع اتصال از لحاظ استفاده از سرویس دائم و پر سرعت باند پهن ADSL و یا اتصال موقت Dial-Up تأثیر

زیادی در ویروسی شدن کامپیوتر شما دارد. در صورتی که از یک اتصال دائم و پر سرعت جهت ورود به دنیای اینترنت بهره می برید طعمهٔ خوبی برای **کرم های اینترنتی** و هدفی مناسب برای **هکرها** می باشید. برای مقابله با این مشکلات بهترین راه، استفاده از یک برنامهٔ پر قدرت محافظ و اسکن اطلاعات کامپیوتر بر اساس یک برنامهٔ مدون به وسیلهٔ برنامهٔ ویروس‌یاب می باشد.



داشتن یا نداشتن فایروال

فایروال در واقع یک **دیوار مجازی امنیتی** برای جلوگیری از نفوذ ویروس ها، کرم ها و اسب های ترویا به کامپیوتر می باشد. استفاده از فایروال های نرم افزاری یا سخت افزاری یکی از ایده آل ترین روش های محافظت از کامپیوتر در مقابل خطرات در کمین نشسته می باشد.

برنامه های فایروال در پشت صحنه کامپیوتر شما همانند یک گارد محافظتی عمل می کنند و به **بررسی دقیق ارتباطات** یک کامپیوتر می پردازند. فایروال‌ها به دو صورت نرم‌افزاری و سخت‌افزاری قابل استفاده هستند.



فایروال های سخت افزاری در واقع یک **قطعهٔ الکترونیکی** می باشد که در روی شبکه نصب می‌شوند و مشابهٔ برنامه های نرم افزاری فایروال عمل می کنند با این تفاوت که حفاظت بهتری را بر روی تمام کامپیوترهای تحت شبکه اعمال می کنند.

خطر کردن در مقابل ویروس ها

شرایط و کارهای خاصی احتمال ویروسی شدن کامپیوتر شما را ، تا حد زیادی بالا می برد که از آن جمله می توان:

☜ **دانلود کردن و به اشتراک گذاری فایل ها:** در صورتی که شما عادت به دانلود کردن برنامه ها و اطلاعات مختلفی از اینترنت دارید، باید **مراقب ویروس های** در کمین نشسته برای رسوخ به کامپیوترتان باشید. چه بسا با دانلود یک فایل، ویروسی خطرناک را نیز به کامپیوتر خود کپی کنید.

☜ **پیغام های فوری:** استفاده از برنامه های پیغام رسان فوری، امکان ویروسی شدن کامپیوتر شما را به سادگی فراهم می کنند. **کرم ها** و **ویروس های** زیادی از طریق پیغام رسان های تحت اینترنت به صورت سریع گسترش می یابند.

☜ **اضافه کردن برنامه:** یکی دیگر از روش های تکثیر و انتقال ویروس ها، نصب و راه اندازی برنامه های مختلف کامپیوتری می باشد. ویروس ها از طریق نصب برنامه های مختلف می توانند به کامپیوترها نفوذ کرده و اهداف مخرب خود را به سادگی دنبال کنند.

☜ **در اختیار گذاشتن آدرس E-mail:** با انتشار آدرس E-mail خود در بین مردم، شما ضریب آسیب پذیری و ویروسی شدن کامپیوتر خود را تا حد زیادی بالا می برید. افراد ماجراجو با ارسال E-mail ویروس ها و برنامه های مخرب زیادی را با عناوین تحریک کننده برای شما می فرستند و فقط کافی است یکی از این E-mail ها را باز کنید.



بیشتر بدانیم: سریع ترین ویروس کامپیوتری!

یکی از ویروس های کامپیوتری که در حداقل زمان، حدود ۳۰۰ میلیون کامپیوتر را آلوده کرده ویروس I Love You می باشد. علت مهم موفقیت در گسترش و آلوده سازی E-mail های حامل این ویروس را می توان عنوان اغوا کنندهٔ این پیغام (I Love You) دانست.

اینترنت بی سیم: کامپیوترهای دستی و کیفی در هنگام استفاده از اینترنت قربانیان مناسبی برای اسب های ترویا و کرم ها می باشند.

گام دوم: نشانه‌های ویروسی شدن؟

در این گام ما قصد داریم به عنوان اصلی این فصل اشاره داشته باشیم. آیا کامپیوتر شما آلوده به ویروس است؟ و یا بهتر آن است بگوییم که آیا شما می ترسید که کامپیوترتان ویروسی باشد؟

قربانیان ویروس‌ها دارای نشانه‌های مختلفی هستند. اولین نشانهٔ قابل استناد **سر زدن رفتارهای عجیب** از کامپیوتر می باشد. این رفتار عجیب و غریب می تواند ناشی از وجود و عملکرد ویروس ها باشد. دراین قسمت ما قصد داریم نشانه های رایج ویروسی شدن کامپیوتر را گام به گام با هم بررسی کنیم.

کند شدن کامپیوتر

یکی از رایج ترین نشانه های ویروسی بودن کامپیوتر، کند شدن بیش از اندازهٔ کامپیوتر می باشد. البته این موضوع را مد نظر داشته باشید که ویروسی بودن تنها یکی از دلایل کند بودن کامپیوترها است.

در زیر ما به بعضی از دلایل رایج کند شدن کامپیوتر اشاره می کنیم:

- **آیا شما برنامه ای را به روز کرده اید؟** همانند سیستم عامل های جدید، نسخهٔ جدید بعضی از برنامه های نرم افزاری همانند فتوشاپ جهت کار به حافظهٔ بیشتری نیاز دارند.
- **آیا اخیراً شما مقدار زیادی عکس و اطلاعات از اینترنت دانلود کرده اید؟** فایل های تصویری و موسیقی به فضای زیادی جهت ذخیره سازی نیاز دارند. در صورتیکه اخیراً مقدار زیادی از این فایل ها را به کامپیوتر خود دانلود کرده اید ممکن است با کاهش سرعت کامپیوتر روبرو شوید.



در صورتیکه هیچکدام از این دلایل برای کند شدن کامپیوتر شما مصداق نداشت با عرض پوزش باید گفت که **متأسفانه کامپیوتر شما ویروسی است.** لازم نیست عصبی شوید اتفاق هیچ وقت خبر نمی کند!



فعالیت های غیر قابل توضیح

آیا چراغ هارد دیسک شما بدون هیچ دلیلی روشن و خاموش می شود؟ یکی از دلایل این فعالیت های غیر معمول ناشی از ویروس ها و برنامه های مخرب می باشد. هکرها با نفوذ به کامپیوتر شما به فعالیت‌هایی به شرح زیر دست می زنند:

☑ هکرها از کامپیوتر شما جهت **ارسال** صدها یا میلیون ها **اسپم** استفاده کرده و آنها را به همهٔ آدرس های E-mail دوستان شما ارسال می کنند.

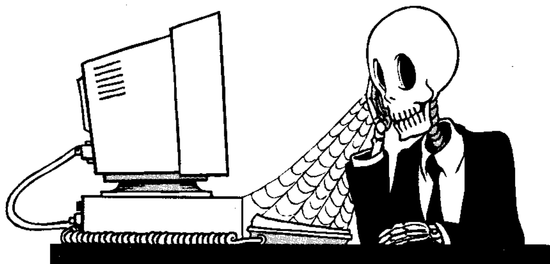
☑ هکرها از کامپیوتر شما به عنوان یک **ستاد عملیاتی جهت حمله** به کامپیوترها و شبکه های مختلف استفاده می کنند. مثلاً در حملهٔ DDOS هکرها با دستور حمله به کامپیوترهای Zom bie (کامپیوتری قربانی مثل شما) به یک وب سایت، انبوهی از پیغام را به سایت مربوطه ارسال می کنند تا با حجم بالای ترافیک، عملکرد سایت مربوطه را فلج سازند.

☑ هکرها با نصب برنامه های جاسوسی اقدام به ارسال اطلاعات کامپیوتر قربانی می کنند. به طور مثال برنامهٔ Key Logger کلیهٔ اطلاعات مربوط به صفحه کلید شما را به صورت مخفیانه **جاسوسی** می کند. این اطلاعات شامل رمز کارت اعتباری شما و کلمهٔ عبور کامپیوتر می باشد.



قفل کردن کامپیوتر!

آیا کامپیوتر شما به صورت مکرر قفل می کند؟ و آیا شما برای این قفل کردن های مکرر توضیحی دارید؟ آیا یک صفحهٔ آبی رنگ در روی صفحهٔ نمایش شما ظاهر می شود؟
قفل کردن کامپیوتر و ظاهر شدن صفحهٔ آبی، اگر مکرراً برای کامپیوتر شما اتفاق بیافتد متأسفانه می توان آنرا ناشی از آلوده شدن کامپیوترتان به وسیلهٔ ویروس ها دانست.



فعال نشدن کامپیوتر

واقعاً که خیلی ناامید کننده است وقتی کلید روشن کردن کامپیوتر را در یک صبح آفتابی فشار دهید و کامپیوتر شما فعال نمی گردد، در این مواقع تنها راه باقی مانده فشار کلید میانبر Ctrl+Alt+Del می باشد. اولین احتمالی که در این مواقع به ذهن شما خطور می کند ویروسی بودن کامپیوتر می‌باشد.
این احتمال هم درست و هم در بعضی مواقع نادرست می باشد. برای این عدم فعالیت می توان دلایل مختلفی مثل خراب بودن سیستم عامل، هارد دیسک، کارت گرافیکی یا RAM ذکر کرد. ولی با تمام این احوال ویروس ها نیز می توانند از فعال سازی کامپیوتر شما جلوگیری کنند.

سرزدن رفتارهای عجیب و غریب از کامپیوتر

گاهی اوقات شما در کامپیوتر خود رفتارهای عجیب و غریبی را مشاهده می کنید. بعضی از این رفتارهای عجیب (البته فقط بعضی) را می توان به ویروسها نسبت داد. نمونه ای از این رفتارها می‌تواند به تغییر ناگهانی موضوعات در صفحهٔ نمایش یا حرکت یک کلمه یا حرف در صفحهٔ نمایش اشاره کرد. تعدادی از این رفتارهایی که ناشی از عملکرد ویروس ها می باشد به شرح زیر می باشد:

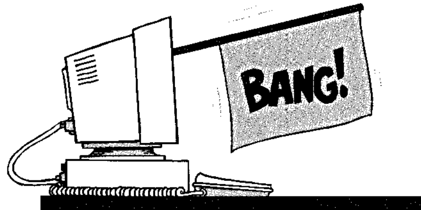
☑ **فایل ها در محل ذخیره سازی خود نیستند و شما نمی توانید آنها را پیدا کنید.** مثلاً یکی از ویروس های ارائه دهندهٔ این عملکرد ویروس **مثلث برمودا** می باشد.

☑ **من فایل های خود را پیدا کردم ولی حجم و نشانه های فایل ها تغییر پیدا کرده است!** بعضی از ویروس ها با آلوده کردن فایل های اطلاعاتی حجم و اندازهٔ آنها را کم و یا زیاد می کنند و ویژگی های فایل را تغییر می دهند.

☑ **متن ها و نوشته های روی صفحهٔ نمایش شروع به تغییر می کنند!**

☑ **پیغامی در روی صفحهٔ نمایش ظاهر می شود!**

بعضی از ویروس ها، پس از آلوده سازی و تخریب یک سیستم کامپیوتری پیغامی مثل «**کامپیوتر شما حالا به یک آشغال تبدیل شده**» را در روی صفحهٔ نمایش ظاهر می کنند. در این مواقع اعصاب کاربر کاملاً به هم می‌ریزد ما به شما حق می‌دهیم.



وجود پنجره های فعال زیاد در روی صفحهٔ نمایش

هنگام کار با کامپیوتر و جستجو در اینترنت، شما احتمالاً با پنجره های فعال زیادی در روی صفحهٔ نمایش روبرو می شوید در حالیکه نیازی به هیچکدام از آنها ندارید (این پنجره ها شامل کادرهای محاوره ای تغییر پیکربندی کامپیوتر، دانلود و ... می باشد).



خلاصهٔ این فصل

این فصل را ما با یک سئوال شروع کردیم «آیا کامپیوتر من ویروسی است؟!» و با برداشتن دو گام جواب هایی را برای این سئوال پیدا کردیم. استدلال های ذکر شده در این فصل کاملاً مستدل می باشد. امیدواریم که شما هم مانند ما با دلایل ارائه شده به جواب سئوال رسیده باشید.

سئوالات تستی

فایروال را تعریف کنید؟

الف: یک سپر دفاعی در مقابل هکرهاست

ب: یک دیوار مجازی امنیتی در کامپیوترهاست

پ: عاملی بازدارنده برای جلوگیری از ورود ویروس ها و هکرها به کامپیوتر می باشد

ج: همهٔ موارد صحیح است

چند نمونه از فعالیت های عجیب و غریبی که دلیل بر ویروسی بودن کامپیوتر شما است را بنویسید؟

الف: کند شدن کامپیوتر

ب: فعالیت های بدون دلیل

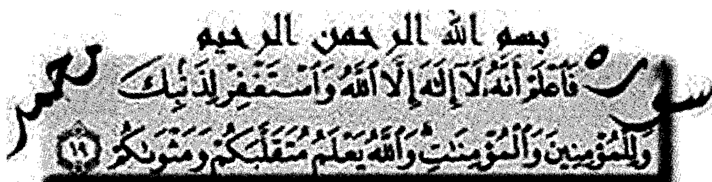
پ: گزینهٔ الف و ب+ فعال شدن کامپیوتر

ج: هیچکدام

«سخنان درگوشی»

آشنایی با یک ویروس جالب

چند سال پیش ما یک ویروس از نوع کرم‌های رایانه‌ای به نام W32/Hosin از نوع وطنی آشنا شدم. اندازهٔ این ویروس ایرانی در حدود ۴۸ تا ۱۶۸ بایت بود که از طریق فلاپی‌دیسک‌ها تکثیر می‌شد و تمامی فایل‌های فلاپی‌دیسک را مخفی می‌کرد. ویروس فوق دارای ۳ نسخهٔ مختلف است. در داخل آخرین نسخهٔ این ویروس دو عکس به شرح زیر وجود دارد.



فصل ۳

هکرها

هکرها افرادی کنجکاو و با هوشی هستند که علاقهٔ فراوانی به نفوذ در کامپیوترهـای دیگـران دارنـد. این افراد با نفوذ به کامپیوترها و شبکه های کامپیوتری اهداف مختلفی را که نـشأت گرفتـه از انگیـزه های مختلف است دنبال می کنند. در این فصل ما قصد داریم از پنجره ای تازه به هکرها نگاه کنـیم و با اهداف و انگیزه های مختلف این افراد آشنا شویم.
دنیای هکرها دنیایی است بی حـد و مـرز کـه گـاهی دردسـرهای زیـادی را بـرای همـسایگان ایجـاد می‌کنند. پس برای داشتن محیطی امن و بی خطر این فصل را به دقت مطالعه کنید. شناخت ایـن افـراد ماجراجو، علایق و انگیزه های آنها به شما در محافظت صحیح در مقابل خطرات پنهانی کمک شایانی می نماید.

گام اول: آشنایی با هکرها

هکرها را می توان بر اساس انگیزهٔ آنها جهت نفوذ به شبکه ها و کامپیوترهـا بـه چنـد دسـته تقـسیم کرد. بر اساس یک باور قدیمی نیاز، انگیزه را پدید می آورد و انگیزه موجب کشف و اختراع می‌گردد. پس شناخت انگیزهٔ نفوذ هکرها را می توان یکی از اولین قدم های مقابله با هکرها دانست.

هکرهای جوانمرد

این هکرها که به هکرهای **سامورایی** نیز معروف هستند اعتقاد به آزادی اطلاعات برای همه را دارنـد و هیچگونه هدف تخریبی خاصی را دنبال نمی کنند. این گروه با نفوذ خود می خواهند به همـه اعـلام کنند که هیچ حد و حصری برای دسترسی به اطلاعات وجـود نـدارد. ایـن گـروه از هکرهـا را تقریبـاً می‌توان بی آزارترین نوع هکرها دانست.



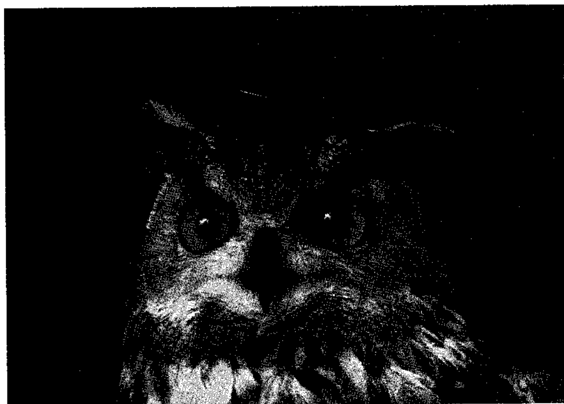
کراکرها

این هکرها که به هکرهای **گانگستر** نیز معروف هستند، دارای اهدافی مخرب با انگیزه های مختلف مالی و ... می باشند. این گروه از هکرها با نفوذ به کامپیوتر دیگران، از اطلاعات موجود کامپیوتر قربانی تا حد ممکن بهره برده و دست به عملیات تخریبی می زنند. این گروه از هکرها را می توان خلافکاران خرده پا دانست که با استفاده از تکنیک های تکراری و برنامه های از پیش تعریف شده و پیش پا افتاده، اقدام به نفوذ می کنند.



واکرها

این هکرها که به **تروریست های اینترنتی** مشهور هستند دارای مهارت ها و تکنیک های منحصر به فردی جهت نفوذ به سایت ها، کامپیوترهای شبکه و سرورهای مهم هستند. این گروه از هکرها با نفوذ به شبکه های کامپیوتری اهداف مختلف **سیاسی**، **مالی** و **اعتقادی** خود را دنبال می کنند. این گروه از هکرها افراد متخصصی هستند که از روش های منحصر به فردی برای نفوذ به سایت ها بهره می برند بنابراین شناسایی و برخورد با آنها بسیار مشکل می باشد. این دسته از هکرها را می‌توان خطرناک ترین نوع هکرها دانست.



بیشتر بدانیم: مشتریان پر و پا قرص کراکرها چه کسانی هستند؟

تخصص بالای بعضی از این کراکرها باعث گردیده که بعضی از شرکت ها برای محافظت از شبکه های کامپیوتری خود از آنها بهره ببرند چون آنها به این ضرب المثل اعتقاد دارند که پلیسی می تواند بهترین پلیس باشد که در درجهٔ اول دزد خوبی باشد. ضمناً بعضی از این شرکت ها جهت ضربه زدن به شرکت های رقیب از این هکرها استفاده می کنند.

در دنیای امروز کار این دسته از هکرها بسیار گرفته است به طوریکه بعضی از آنها به استخدام سازمان های بزرگ جاسوسی مثل **سیا** و **موساد** در آمده اند. مثلاً در جریان جنگ آمریکا علیه عراق کراکرهای این سازمان های جاسوسی با نفوذ به وب سایت شبکهٔ الجزیره و تغییر اطلاعات آن، چند روز در روند اطلاع رسانی این شبکهٔ خبررسانی اختلال ایجاد کردند.

کدام یک بهترند؟

این سئوالی است که ممکن است در ذهن شما نقش بسته باشد. باید در جواب آن گفت که نفوذ به حریم امن و خصوصی اطلاعاتی دیگران با هر هدف و انگیزه ای (هر چند انسانی) کاری غیر اخلاقی است. از هک کردن دیگران می توان، این طور استناد کرد که شما به بهانهٔ کنجکاوی پاک و بی‌نظر، مخفیانه به منزل فرد دیگری وارد شوید. احترام به حریم خصوصی دیگران یکی از اصول داشتن دنیایی سالم و پاک می باشد.



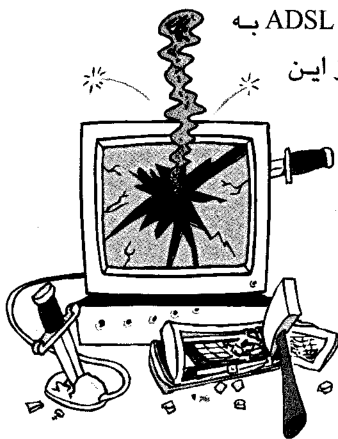
گام دوم: مفاهیم اساسی هک

در برخورد با هکرها و روش های نفوذ آنها شما احیاناً با اصطلاحاتی برخورد می کنید که ممکن است برای شما تازگی داشته باشد. در این گام ما به همراه هم قصد داریم نگاهی گزینشی به این مفاهیم داشته باشیم.

IP چیست؟

IP در واقع آدرسی است که به هر کاربر جهت شناسایی در اینترنت اختصاص داده می شود. IP اختصاصی به هر فرد شامل چهار قسمت مجزا می باشد مثلاً هنگامی که شما به اینترنت وارد می‌شوید ممکن است آدرس IP به این شکل داشته باشید: 881.56.822.421

چرا یک کامپیوتر استفاده کننده از خطوط پرسرعت، خوراک مناسبی برای هکرهاست؟



همانطور که قبلاً نیز به آن اشاره شد خطوط پرسرعت DSL یا ADSL به صورت دائم به اینترنت متصل می باشد بنابراین استفاده کننده از این خطوط دارای یک آدرس IP ثابت می باشد (برخلاف سرویس های Dial-Up که با هر بار اتصال دارای یک IP جدید هستند). از این رو هکرها با شناسایی کامپیوترهای استفاده کننده از خطوط پرسرعت و **شناسایی IP** آنها به راحتی به کامپیوترشان نفوذ می‌کنند.



گام سوم: آشنایی با انواع برنامه‌های هک

خوشبختانه تعداد افرادی که از برنامه های آمادهٔ هک استفاده می کنند نسبت به هکرهای خود ساخته بسیار بیشتراست. در این گام ما قصد داریم نگاهی گذرا به مهمترین برنامه های هک داشته باشیم.

برنامه های گزارش دهندهٔ صفحه کلید



این دسته از برنامه ها را می توان جزء برنامه های جاسوسی دانست که کلمات عبور، نوشته های تایپ شده و مکالمات شما را در اتاق های چت را به هکرها گزارش می کنند.

این گزارشات شامل شماره و رمز کارت اعتباری شما، رمز ورود به شبکه و ... می باشد.

برنامه های بازیابی کنندهٔ کلمات رمز

بعضی از هکرها با نفوذ به کامپیوتر شما به وسیلهٔ برنامه های بازیابی کننده می توانند به کلمهٔ رمز شما، صندوق پستی ، حساب بانک، شبکه و ... شما دسترسی پیدا کنند.

برنامه های کنترل کننده

بعضی از برنامه ها با نفوذ به کامپیوتر قربانی، کنترل عملکردهایی مثل حرکت ماوس و باز و بسته شدن CD-Rom و یا کنترل صفحهٔ رومیزی را به دست می گیرند. هکرهای استفاده کننده از این برنامه ها ممکن است آسیب جبران ناپذیری را به اطلاعات کامپیوتر شما وارد کنند.





بمب ایمیل

یکی از برنامه های رایج که هکرها برای پر کردن صندوق پستی شما و نهایتاً فلج کردن آن مورد استفاده قرار می دهند بمب های ایمیل می باشد.

هک به وسیلهٔ ویروس ها

یکی از روش های تخریب اطلاعات به وسیلهٔ هکرها استفاده از برنامه های مخرب و ویروس می‌باشد. به این صورت که هکر با نفوذ به کامپیوتر قربانی و قرار دادن یک ویروس یا برنامهٔ تخریب در عملکرد کامپیوتر مربوطه ایجاد اختلال می کند. می توان رابطهٔ بین هکرها و ویروسها را ارتباطی تنگاتنگ و خطرناک دانست.



گام چهارم: آیا من هک شده‌ام؟

یکی از نکات مهم در کار با کامپیوتر و شبکه های کامپیوتری، بررسی مدام و همیشگی کامپیوتر می‌باشد. چه بسا ویروسی خطرناک و برنامه‌های جاسوسی که در کامپیوتر شما زندگی شیرینی را سپری می کند و شما از وجود آن بی خبر هستید و در یک فرصت طلایی ضربهٔ هولناکی را به اطلاعات کامپیوترتان وارد می کند. در این گام ما با طرح سئوالی قصد داریم به نگاه شما جهت ببخشیم.

«آیا کامپیوتر من هک شده است؟!» برای پی بردن به جواب این پرسش ما را همراهی کنید.

> ☺ همراه: بسیاری از دلایل ذکر شده زیر با نشانه های ویروسی شدن یک کامپیوتر شباهت زیادی دارد. این مسئله را می توان دلیلی برای نزدیکی فراوان بحث ویروس ها و هکرها دانست.

مشاهدهٔ تغییرات

به تغییرات اعمالی در فایل های اطلاعاتی کامپیوتر خود دقت فراوانی را مبذول دارید چه بسا برنامه‌های مخرب قرار داده شده توسط هکرها، عامل این تغییرات باشند.



فعالیت های غیر قابل کنترل

هنگام استفاده از اینترنت به عملکرد کامپیوتر خود توجه کاملی را مبذول دارید و نسبت به فعالیت های غیر قابل توضیح (مثل باز شدن یک پنجره یا کادر محاوره ای) مشکوک باشید.

کند شدن کامپیوتر

به سرعت مرور صفحات وب در هنگام اتصال به اینترنت توجه خاصی را مبذول دارید. در صورتی که سرعت مرور شما به اینترنت به طرز وحشتناکی کاهش یافت ممکن است مهمان ناخوانده ای در کامپیوتر شما در حال تفریح و جستجو باشد.



> بیشتر بدانیم: ویروسی شدن در حداقل زمان!
>
> حادثه هیچگاه خبر نمی کند و در یک لحظهٔ کوتاه اتفاق می افتد. سفینهٔ فضایی چالنجر در عرض ۷۳ ثانیه بعد از بلند شدن منفجر شد و در عرض دو ساعت و ۴۰ دقیقه کشتی غرق نشدنی و افسانه ای تایتانیک پس از برخورد با کوه یخ در سر و صدای اقیانوس خاموش شد.
>
> این مقدمه برای کامپیوتر و شبکه های کامپیوتری نیز بسیار صادق می باشد. کرم کامپیوتر **Nimdo** در زمانی کمتر از یک ساعت و نیم در تمام دنیا پخش شد و یا کرم **Witty** در عرض ۴۵ دقیقه تمامی سیستم‌هایی در دنیا که قابلیت آلوده شدن را داشتند آلوده کرد.

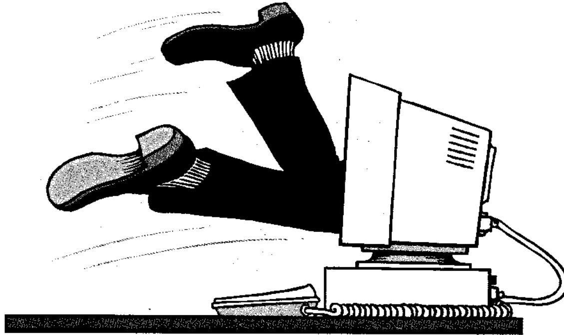
گام پنجم: نحوهٔ مقابله با هکرها

حالا شما دید تازه ای را نسبت به هکرها و انواع آنها پیدا کردید و با نحوهٔ عملکرد کلی آنها آشنا شدید. دراین گام ما قصد داریم به مهمترین بخش این فصل یعنی آشنایی با روش های مقابله با هکرهای کامپیوتری بپردازیم. راهنمایی ها و دستورالعمل‌ها ذکر شده به صورت کلی روش های مقابله با هکرها را مطرح کرده‌اند و می توانند به محافظت کامپیوتر شما در مقابل هکرها کمک شایانی را بکنند.

گول نخورید

در صورتیکه شما مدیر یا کارمند یک شرکت با یک شبکهٔ کامپیوتری هستید باید با ترفندهای هکرها آشنایی کامل داشته باشید. یکی از این ترفندها گول زدن کاربران شبکه، جهت دستیابی به کلمهٔ عبور

می باشد. در اینگونه موارد فرد با ارسال پیغام خود را یک کارمند و همکار جدید معرفی کرده و از شما می خواهد که کلمهٔ عبور شبکه را برای یک پروژهٔ خیلی مهم در اختیار وی قرار دهید و گاهاً با به کار بردن عباراتی چون **پروژهٔ حیاتی** و مهم شما را تحت فشار قرار می دهند. در برخورد با این پیغام ها بسیار حساب شده رفتار کنید.



نصب تنظیمات حفاظتی ویندوز

هنگام مرور صفحات وب، حتماً از تنظیمات حفاظتی ویندوز که به صورت پیش فرض در روی آن قرار گرفته، استفاده کرده و آنها را فعال کنید.

مراقب پیوست E-mail ها باشید!

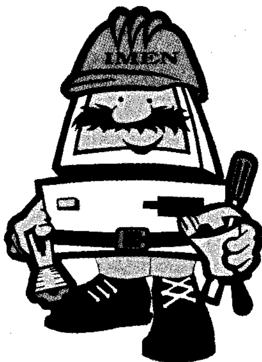
همانند ویروس ها برنامه های جاسوسی جهت گزارش به هکرها در پیوست E-mail ها پنهان می‌شوند و به محض باز شدن پیغام در روی کامپیوتر شما نصب می شوند.



از یک فایروال استفاده کنید!

این راه کار را شاید بتوان بهترین روش مقابله با نفوذ هکرها دانست. همانطور که قبلاً نیز به آن اشاره شده فایروال ها دیوار دفاعی مجازی در مقابل نفوذ هکرها می باشند. در صورتیکه شما مدیر

یک شرکت با اطلاعات ارزشمندی هستید از یک فایروال شناخته شده که امکانات پشتیبانی فراوانی را در اختیار کاربران قرار می دهد استفاده کنید.



به روز سازی فایروال

استفاده از یک فایروال معتبر با امکان به روزسازی قدرت مقابله با انواع خطرات احتمالی را برای شما فراهم می کند. حدالامکان سعی نمایید به روزسازی فایروال کامپیوتر خود را بر اساس یک جدول زمان بندی مشخص انجام دهید. فاصلهٔ زمانی بین هر به روزسازی فایروال به حجم، کیفیت و ارزش اطلاعات کامپیوتر و شبکهٔ شما بستگی دارد. جدول زیر راهنمای مفیدی جهت تنظیم یک برنامهٔ به روز سازی فایروال می باشد:

	امنیت سطح بالا	امنیت سطح متوسط	امنیت سطح پایین
نوع استفاده	اطلاعات محرمانه-حسابداری کلان	مکاتبات خانوادگی-حسابداری معمولی	دریافت ایمیل-بازیهای کامپیوتری-جستجو در وب
مقدار خطر	بالا	متوسط	اندک
به روزسازی ویروس یاب	روزانه	هفتگی	ماهانه

بیشتر بدانیم: هکرها به چه کامپیوترهایی حمله می کنند؟!

هکرهای حرفه ای واقعاً خطرناک، دقیقاً همانند یک دزد حرفه ای عمل می کنند و به کامپیوترهایی حمله می کنند که ارزش اطلاعاتی بالایی (از نظر مادی یا معنوی) داشته باشند. کامپیوترها و شبکه هایی که هدف بسیاری از هکرها می باشند به شرح زیر است:

- شبکه ها و کامپیوترهای سرور بانک ها
- شبکه ها و کامپیوترهای ارگان های دولتی حساس
- کامپیوتر نویسندگان بزرگ مثل جی کی رولینگ (نویسندهٔ کتاب های هری پاتر) جهت سرقت آخرین کتاب آنها

- وب سایت روزنامه های کثیر الانتشار
- وب سایت شبکه های خبری بزرگ
- وب سایت سازمان های سیاسی
- وب سایت های آموزش دهندهٔ مقابله با هکرها

حمله هکرها فقط منحصر به کشورهای خارجی نیست. شما شاید در مورد حملهٔ هکرها در ایران به شبکه های بانکی و سایت خبرگذاری های معتبر شنیده باشید.

خلاصهٔ این فصل

در این فصل ما با یکی از پر صداترین خطرات در کمین نشسته در اینترنت به نام هکرها آشنا شدیم. در این فصل شما مطالب زیادی را در مورد هکرها و نحوهٔ نفوذ و مقابله با آنها یاد گرفتید و در این راه با مفاهیم کاربردی و مهم در درک صحیح هکرها آشنا شدید. همچنین استراتژی ها و برنامه های معروف هکرها را مرور کرده و نحوهٔ پی بردن به وجود آنها را بررسی کردیم. در انتها با کاربردی ترین روشهای مقابله با هکرها به عنوان یک پدیدهٔ غیر قابل اجتناب در دنیای کامپیوتر آشنا شدید.

سئوالات تستی

هکر را تعریف کنید؟

الف: یک فرد ماجراجوست

ب: اصطلاحی در مورد نفوذگرها به کامپیوترهاست

پ: یک فرد کنجکاو است

ج: همهٔ تعاریف فوق برای هکرها صحیح است

آیا می توان عملکرد هکرهای سیاسی (یا واکرها) را توجیه کرد؟

الف: خیر

ب: بله در بعضی از مواقع قابل قبول است

به روز سازی فایروال چه تأثیری در جلوگیری از نفوذ هکرها دارد؟

الف: قدرت تدافعی برنامهٔ فایروال را بالا می برد

ب: قابلیت مقابله با ویروس ها و تکنیک های های جدید هکرها را افزایش می دهد

پ: حملات آنها را ناکام می کند

ج: همهٔ موارد صحیح است

«سخنان درگوشی»

هکرها، شکل یا راه حل

اکثر کاربران کامپیوتر و اینترنت هکرها را مجرمان و متجاوزان به حریم خصوصی دیگران می‌دانند اما شاید باور نکنید که همین متجاوزین امروزه به عنوان آخرین راه‌کار کارآمد برای محافظت و امنیت اطلاعات شناخته شده‌اند!

از این رو شاید وقت آن رسیده باشد که دید خود را نسبت به این افراد متخصص ولی خطرناک، مهربان‌تر کنیم. این موضوع عجیب است ولی واقعیتی است که یکی از دلایل اصلی پیشرفت کامپیوترها و شبکه‌ها همین هکرها هستند. برای تأیید این ادعا همین بس که مؤسسان اصلی شرکت بزرگ کامپیوتری Apple دو هکر به نام‌های استیو جابرْ و استیو وزنیک بوده‌اند و حتی سیستم عامل یونیکس توسط چند هکر حرفه‌ای نوشته و طراحی شده است. هکرها انسان‌هایی باهوش و بعضاً نابغه‌ای هستند که استعدادهای خود را در جهت معکوس به کار گرفته‌اند. بر همین اساس امروزه ما شاهد استخدام هکرها توسط شرکت‌های بزرگ امنیتی و کامپیوتری هستیم، مثلاً در ماه گذشته به دستور اوباما رئیس جمهور آمریکا، معاون وی رابرت گیتس ردیف بودجه‌ای را برای استخدام هکرهای کارکشته در پنتاگون اختصاص داد تا از آنها برای مقابله با حملات سایبری استفاده شود. این نتیجه‌ای منطقی است که هکرها بهترین، مؤثرترین راه‌حل برای حفظ و امنیت اطلاعات هستند.

حالا شما مختارید که از این مجرمان خطرناک و نابغه استفاده کنید و یا قربانی آنها شوید.

فصل ۴

برنامهٔ ضد ویروس

احتیاط شرط عقل است و عاقل کسی است که در مقابل خطرات احتمالی احتیاط را رعایت کند، اما این را هم بدانید که ترس برادر مرگ است. همانطور که در فصل های پیش به صورت مکرر به آن اشاره شد هکرها، ویروس و برنامه های مخرب فرایندی غیر قابل اجتناب در دنیای کامپیوتر می باشند.
برای مقابله با ویروس های کامپیوتری و تهدیدات آنها عاقلانه ترین کار ممکن، مجهز کردن کامپیوتر به یک **برنامهٔ ضد ویروس** می باشد. برنامه های ضد ویروس بهترین گزینه برای مقابله با ویروس های کامپیوتری است.
در این فصل قصد داریم به بررسی برنامه های ضد ویروس و خصوصیات و ویژگی های این برنامه ها بپردازیم و شما را در انتخاب یک برنامهٔ ضد ویروس مناسب یاری دهیم.

گام اول: آشنایی با برنامه‌های ضدویروس

امروزه واژهٔ نرم افزار مترادف با برنامه های کامپیوتری مورد استفاده قرار می گیرد. یک برنامه در واقع مجموعه ای از دستورالعمل ها و باید یا نباید هاست. ولی نرم افزار جزئی از یک مجموعه برنامهٔ طراحی شدهٔ متناسب با یکدیگر می باشد. ویروس های کامپیوتری را می توان نوعی نرم افزار کثیف و غیر مجاز دانست که به تنهایی می تواند به تخریب و انهدام اطلاعات کامپیوتر بپردازد.



برنامه های ضد ویروس به صورتی طراحی شده اند تا کامپیوتر شما را از دست ویروس های کامپیوتری نجات دهند و اغلب از سه روش جهت مقابله استفاده می کنند:

☑ شناسایی ویروس های موجود کامپیوتر شما

☑ جلوگیری از فعالیت های مخرب آنها

☑ حذف ویروس ها

آیا در کامپیوتر من برنامهٔ ضد ویروس وجود دارد؟

شاید تعجب کنید ولی ممکن است برنامهٔ ضد ویروس قبلاً بر روی کامپیوتر شما نصب شده باشد، بدون اینکه شما از وجود آن اطلاع داشته باشید.

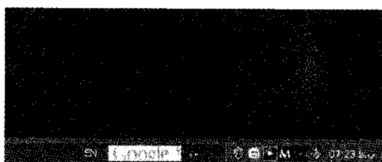


آیکون های مربوط به برنامه های ضد ویروس در قسمتهای مختلفی از کامپیوتر شما قابل دسترس می باشد. بعضی از این آیکون ها در منوی Start، بعضی در روی صفحهٔ رومیزی و بعضی دیگر در کنار ساعت کامپیوتر شما وجود دارند.

نگاهی به کنار ساعت کامپیوتر خود داشته باشید!

همانطور که ذکر گردید به عنوان اولین گام جستجوی برنامهٔ ضد ویروس نگاهی به کنار ساعت برای مشاهدهٔ آیکون برنامهٔ ضد ویروس داشته باشید. ساعت کامپیوتر به صورت پیش فرض، در سمت چپ نوار کار کامپیوتر شما قرار گرفته است. البته نوار کار کامپیوتر می تواند به صورتی تنظیم شود تا در زمان قرار گرفتن مکان نمای ماوس روی آن آشکار و به محض قرار گرفتن مکان نمای ماوس در روی صفحهٔ رومیزی پنهان گردد.

در جدول زیر آیکون اکثر برنامه های ضد ویروس رایج که شما می توانید در کنار ساعت کامپیوتر خود مشاهده کنید آمده است:



آیکونی که شما می بینید	ضد ویروس
	Symanten
	Panda
	ایمن
NORMAN	Norman
F-SECURE	F-Secure
PC-cillin	Pc-cillin
M	Mc-Afee
	Avira

☺ همراه: در صورتی که هیچ آیکون ضد ویروسی در کنار ساعت کامپیوتر خود مشاهده نکردید ممکن است:

☑ برنامهٔ ضد ویروس با سیستم عامل شما هماهنگ نباشد.

☑ برنامهٔ ضد ویروس فعال نباشد.

☑ ویندوز شما به تنظیماتی خاص نیاز داشته باشد.

گام دوم: بررسی وضعیت عملکرد برنامه‌های ضدویروس

پس از پیدا کردن برنامهٔ ضد ویروس در روی کامپیوتر خود، شما نیاز دارید نگاه دقیق تری را به برنامه داشته باشید. بعد از کسب اطلاعات لازم در مورد نصب برنامهٔ ضد ویروس بر روی کامپیوتر خود، باید تنظیماتی را بر روی برنامهٔ ضد ویروس انجام دهید. این تنظیمات شامل:

☑ اولویت بندی و تنظیم برنامهٔ ضد ویروس

☑ کشف دقیق عملکرد و پیکربندی قابلیت های برنامهٔ ضد ویروس

☑ تشخیص این که ضد ویروس هنگام فعال شدن کامپیوتر عمل می کند

بعد از روشن کردن کامپیوتر و فعال شدن سیستم عامل، تعدادی از برنامه ها به صورت خودکار فعال گردیده و شروع به کار می کنند. برنامه های ضد ویروس در این زمان به اشکال مختلفی شروع به کار می کنند. برای تشخیص فعالیت برنامه های ویروس یاب به نکات زیر توجه فرمایید:

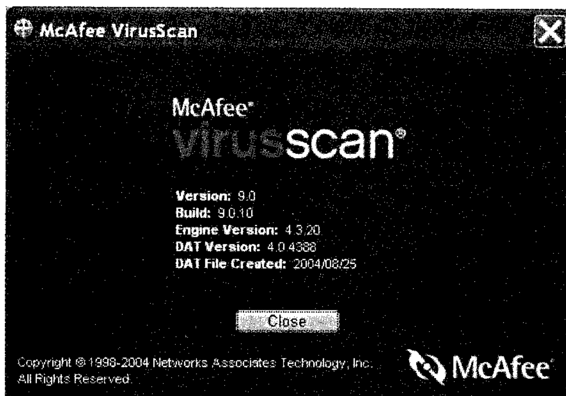
☜ **بررسی پنجرهٔ اعلان فعالیت:** در هنگام شروع به کار ویندوز، پنجره ای فعالیت برنامهٔ ضد ویروس را اعلام می کند. عمر مفید این پنجره چیزی در حدود ۱۰ ثانیه است و حاوی عبارتی مثل «به من نگاه کن من فعال شدم» می باشد.



☜ **بررسی آیکون های کنار ساعت:** یکی دیگر از علایمی که شما می توانید برای فعال سازی برنامهٔ ضد ویروس به آن توجه کنید آیکون و شکل آن در کنار ساعت کامپیوتر می باشد.

تشخیص نسخهٔ برنامهٔ ضد ویروس

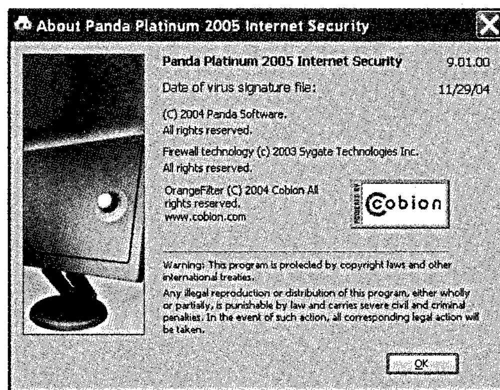
برای تشخیص نسخهٔ برنامهٔ ضد ویروس، پنجرهٔ اصلی برنامهٔ ویروس یاب را فعال کرده و دستور Help→About را انتخاب کنید و در پنجرهٔ ظاهر شده به اسم دقیق و نسخهٔ آن دست یابید.



مشخص کردن آخرین زمان به روز رسانی

یکی از نکات مهم که هنگام استفاده از برنامه های ضد ویروس توجه خاصی را باید به آن مبذول کرد به روز بودن برنامهٔ ضد ویروس می باشد. استفاده از برنامه هایی که دارای اطلاعات جدید و به روز نیستند خطرات جبران ناپذیری را به دنبال خواهد داشت.

یکی از امتیازات یک ضد ویروس خوب را می توان به روز بودن اطلاعات و شناسایی ویروس های جدید دانست. یک برنامهٔ ضد ویروس به روز نشده در مقابله با ویروس های جدید هیچ قدرت دفاعی ندارد.



مشخص کردن آخرین اسکن انجام شده

راستی آخرین باری که شما اطلاعات خود را به وسیلهٔ برنامهٔ ویروس یاب اسکن کرده اید چه زمانی بوده است؟!

☺ همراه: به بررسی و جستجوی اطلاعات کامپیوتر اصطلاحاً **اسکن** می گویند.

یکی از مسائل مهم که در ویروس یابی به آن توجه خاصی را باید مبذول کرد استفاده از یک برنامهٔ زمان بندی منظم جهت اسکن اطلاعات کامپیوتر توسط برنامهٔ ویروس یاب می باشد.
فاصلهٔ زمانی بین هر بار اسکن به عوامل مختلفی بستگی دارد که از آن جمله می توان به **حجم و ارزش اطلاعات** کامپیوتر اشاره کرد.

گام سوم: توجه به قابلیت‌های مهم برنامه‌های ضد ویروس

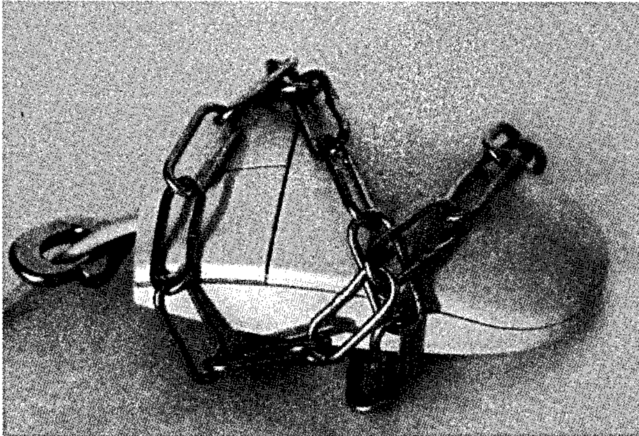
در صورتیکه هنگام خرید یک برنامهٔ ضد ویروس، اطلاعات زیادی را در مورد نوع و قابلیت این نوع برنامه ها ندارید بهتر است از تجربیات دوستان و راهنمایی های فروشندهٔ این برنامه ها نهایت استفاده را بکنید (انتخاب خود را به یک یا دو فروشنده محدود نکنید). تا می توانید سئوال کنید و مطمئن باشید که همیشه حق با مشتری است.

یکی دیگر از بهترین منابع اطلاعاتی یک برنامهٔ ضد ویروس، **وب سایت** مربوط به آن است. در این وب سایت ها شما می توانید به اطلاعات جامع و کاملی در مورد برنامهٔ ضد ویروس و قابلیت های آن دست یابید. در این گام ما عناوینی که فکر می کنیم درانتخاب یک برنامهٔ ویروس یاب مهم است را آورده ایم امیدواریم که هنوز از همراهی با ما خسته نشده باشید:



رایگان بودن یا نبودن برنامهٔ ضد ویروس

یکی از مهمترین قابلیت های یک برنامهٔ ضد ویروس را می توان امکان دانلود قابلیت های جدید برنامه از طریق اینترنت و اضافه کردن به آن دانست. یکی از عوامل تأثیر گذار در قیمت یک برنامهٔ ضد ویروس را می توان داشتن یا نداشتن این قابلیت دانست. زیرا برنامهٔ ضد ویروس بدون داشتن قابلیت اضافه شدن و دانلود اطلاعات و به روزسازی از طریق اینترنت در مقابل نسل های جدید ویروس ها کاملاً آسیب پذیر می باشد.



اکثر برنامه های ویروس یابی معتبر به شما امکان استفاده از خدمات پشتیبانی Online و رایگان را حداقل تا یک سال می دهند. بعضی از برنامه های ویروس یاب غیر معتبر که اکثر آنها نیز به صورت رایگان (یا با قیمت بسیار ارزان) می باشند هیچکدام امکان استفاده از خدمات پشتیبانی را به شما نمی‌دهند.

متأسفانه استفاده از این برنامه های ضد ویروس تا حد زیادی در کشور ما رو به گسترش می باشد. در حالی که شما با صرف هزینه ای اندک می توانید صاحب یک برنامهٔ ضد ویروس معتبر شوید.

دسترسی سریع به قابلیت ها

یکی از ویژگی های مهم برنامه های ضد ویروس که می توان به آن اشاره کرد سادگی کار با این برنامه ها می باشد. شاید بتوان یکی از ویژگی های یک برنامهٔ ضد ویروس ایده آل را **سادگی استفاده** از راهنماهای پنجرهٔ برنامه جهت اسکن فایل ها، دایرکتوری ها و اطلاعات کامپیوتر دانست. مثلاً یکی از ویژگی های جالب در بعضی از برنامه های ضد ویروس، اسکن فایل ها و دایرکتوری ها با راست کلیک کردن روی آنها می باشد.

سازگاری با برنامهٔ ارسال و دریافت E-mail

یکی دیگر از پارامترهای قابل تأمل در انتخاب بهترین برنامهٔ ویروس یاب، هماهنگی برنامهٔ انتخابی با برنامهٔ ارسال و دریافت E-mail می باشد. خوشبختانه اکثر برنامه های ضد ویروس امروزی دارای قابلیت اسکن E-mail های دریافتی می باشند. متداول ترین روش های ارسال و دریافت E-mail ها به دو صورت زیر می باشد:

☜ **سرویس دهندهٔ E-mail محلی:** در صورتیکه شما از یک سرویس دهندهٔ E-mail محلی مثل Outlook Express استفاده می کنید که مستقیماً امکان اتصال و ارسال E-mail در اینترنت را برای شما فراهم می کنند. مطمئن باشید که برنامهٔ ضد ویروس تمام E-mail های دریافتی شما را بررسی می کند.

☜ **سرویس دهندهٔ E-mail تحت وب:** استفاده از مرورگر وب جهت ارسال و دریافت E-mail امروزه بسیار گسترش پیدا کرده است و متأسفانه برنامه های ضد ویروس در اسکن این e-mailها ناتوان می باشند. شاید علت این امر را بتوان عدم ذخیره سازی E-mail های ارسالی برای شما در کامپیوترتان عنوان کرد. کلیهٔ E-mail های ارسالی برای شما در وب سایت ارائه دهندهٔ آنها ذخیره می باشد.



به روزسازی قدرت تدافعی

قابلیت به روزسازی برنامهٔ ضد ویروس یکی از عملکردهای قابل تأمل در انتخاب یک برنامهٔ مناسب می باشد. به روزسازی را می توان یک **سوپاپ اطمینان** برای کارآمدی همیشگی برنامه های ضد ویروس دانست. اکثر برنامه های ضد ویروس خوشبختانه امروزه مجهز به قابلیت به روزسازی

اتوماتیک می باشند که این کار را به صورت روزانـه، شـبانه، دوبـار در روز و حتـی سـاعتی انجـام می‌دهند.

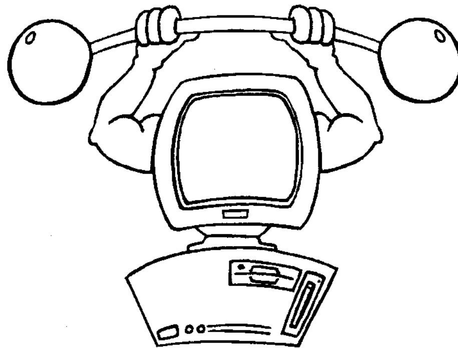
گام چهارم: دسته‌بندی دیگر جزئیات

نسخهٔ کامل یک برنامهٔ ضد ویروس شامل ابزارها و امکانات مختلفی مثل ضد اسپم، فایروال و بلوکه کنندهٔ تبلیغات ناخواسته نیز می باشد. در این گام ما قصد داریم نـیم نگـاهی بـه ایـن جزئیـات داشـته باشیم.

بلوکه کردن کرم ها و هکرها به وسیلهٔ فایروال

یکی از گاردهای حفاظتی برای داشتن یک محیط امن در اینترنت، فایروال ها می باشند. فایروال ها را می توان ابزاری مهم جهت جلوگیری از نفوذ هکرها به کامپیوترها و دستکاری اطلاعات توسـط آنهـا دانست.

فایروال ها مسیرهای دفاعی را جهت جلوگیری از این خطرات در روی کامپیوتر شما قرار می دهند و هنگام بروز خطر به وسیلهٔ علائمی هشدار دهنده به شما اطلاع می دهند.



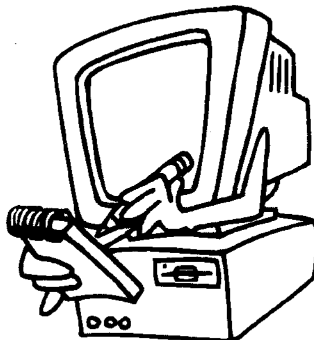
از بین بردن اسپم ها

اگر شما از آن دسته از افرادی هستید که هر روز یک دو جین از E-mail های ناخواسته یا اسـپم هـا را دریافت می کنید این قسمت را به دقت مطالعه نمایید.

برنامه های ضد ویروس برای از بین بردن اسپم ها از روش هایی به شرح زیر بهره می برند:

☜ **با استفاده از کلید واژه:** برنامه های ضد اسپم، جستجوی خود را بـر اسـاس کلمـات و عبـارات کلیدی در پیغام های رسیده انجام می دهند. هر پیغامی که حاوی کلید واژه های تعریـف شـده باشـد بلوکه می شود.

☜ **به وسیلهٔ لیست سفید:** لیست سفید را می توان مقابل لیست سیاه دانست. در این لیست مجموعه آدرس های افراد مجاز به ارسال پیغام برای شما وجود دارد. در صورت تطابق پیغام های رسیده با محتویات لیست سفید اجازهٔ دریافت صادر می گردد.



☺ همراه: متأسفانه در صورتیکه از یک سرویس دهندهٔ E-mail تحت وب بهره می برید نمی توانید از برنامه های ضد اسپم بهره ببرید.

از بین بردن پنجره های تبلیغاتی

هنگام مرور صفحات مختلف وب، شما با پنجره های تبلیغاتی روبرو می شوید که به صورت ناخواسته و شناور در روی صفحهٔ نمایش ظاهر می شود و هر کدام سعی دارند کالای مورد نظرشان را تبلیغ کنند. این پنجره های تبلیغاتی با بالا بردن ترافیک، سرعت مرورگر شما را کاهش داده و جلوی دید شما را می گیرند. خوشبختانه اکثر برنامه های ضد ویروس امکاناتی را جهت بلوکه کردن این تبلیغات مزاحم در اختیار شما قرار می دهند.

خنثی سازی برنامه های جاسوسی

همانطور که قبلاً نیز به آن اشاره شد برنامه های جاسوسی را می توان نوعی از نرم افزارهایی دانست که اغلب به وسیلهٔ هکرها جهت بررسی و گزارش اطلاعات حیاتی و مهم کامپیوتر مورد استفاده طراحی می گردند. با داشتن یک برنامهٔ بلوکه کننده، شما لازم نیست دیگر نگران این برنامه ها باشید.

شاید برای شما باور کردنی نباشد اگر بدانید هم اکنون برنامه ای جاسوسی بر روی کامپیوتر شما نصب شده است. در این قسمت به معرفی چند برنامهٔ ضد جاسوسی می پردازیم:

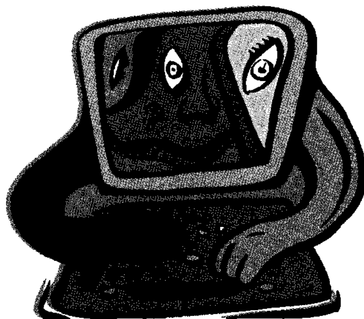
☑ **Ad-Aware:** این برنامه یکی از بهترین برنامه های ضد جاسوسی می باشد.



☑ **Spy bot**: این برنامه با بلوکه کردن کنترل های Active X و Java Script و مرورگر IE بـه مقابلـه با برنامه های ضد جاسوسی می پردازد.

☑ **Spywar Blaster**: این برنامه از ورود نرم افزارهای جاسوسی جلوگیری می کند.

☺ همراه: همهٔ این برنامه ها را می توانید از آدرس **download.com** دانلود کرده و استفاده کنید. همچنین جهت دریافت اطلاعات بیشتر در مورد برنامه های جاسوسی بـه آدرس **www.computervirusesbook.com** مراجعه کنید.



خلاصهٔ این فصل

ما در این فصل تجربه های فراوانی را در مورد برنامه های ضد ویروس و نحوهٔ عملکرد آنهـا کـسب کردیم. با توجه به نکات ذکر شده در این فصل شما می توانید برنامه ای مناسـب و کارآمـد را جهـت مقابله با ویروس ها انتخاب و تهیه کنید.

سئوالات تستی

برنامهٔ ضد ویروس چیست؟

الف: برنامه ای برای بازیابی اطلاعات آسیب دیده

ب: برنامه ای برای بالا بردن قدرت تدافعی

پ: برنامه ای جهت مقابلهٔ کارآمد با ویروس

ج: گزینهٔ ب و پ صحیح است

عوامل مهم در تنظیم یک برنامهٔ مدون به روز سازی ضد ویروس چیست؟

الف: نوع اطلاعات

ب: حجم اطلاعات

پ: ارزش اطلاعات

ج: همهٔ موارد

روش های مورد استفادهٔ برنامه های ضد اسپم را ذکر کنید؟

الف: استفاده از لیست سفید

ب: استفاده از کلید واژه

پ: استفاده از لیست تصاویر

ج: گزینهٔ الف و ب

«سخنان درگوشی»

نگاهی به ویروس‌های ایرانی

تا چند سال پیش ویروس‌های ایرانی، ویروس‌های پرقدرتی نبودند اما حالا ما شاهد تولد ویروس‌های ایرانی هستیم که حتی در سطح بین‌المللی نیز مطرح می‌شوند. به عنوان نمونه‌ای از این ویروس‌ها می‌توان به ویروس سیسیلی، ویروس کاتومیک، ویروس یوسف علی، ویروس قانون، ویروس کولاک و ویروس فووا اشاره کرد.

ویروس کاتومیک که به طور وسیع در بین رسانه‌های عربی مطرح شده دارای نسخه‌های مختلفی است. این ویروس در نسخهٔ A به تبلیغ برای انرژی اتمی پرداخته بود اما در نسخهٔ B ویروس فوق به حمایت از نام خلیج فارس پرداخته بود. از نکات قابل توجه در ویروس‌های جدید ایرانی استفاده از تکنیک‌های مهندسی اجتماعی برای تخریب بود که به عنوان نمونه‌ای از آن می‌توان به ویروس یوسف علی اشاره کرد.

فصل ۵

نصب و نگهداری برنامهٔ ضد ویروس

پس از انتخاب برنامهٔ ضد ویروس جهت استفادهٔ هر چه بهتر از این برنامه، توجه به نکات و تنظیمات هنگام نصب بسیار مهم و اساسی می باشد. عدم توجه به هر یک از نکات کارآیی برنامهٔ ضد ویروس را تا حد زیادی کاهش می دهد.

گام اول: به‌روزسازی برنامهٔ ضد ویروس

همانطور که قبلاً نیز به آن اشاره شد یکی از مهمترین موضوعات جهت مقابلهٔ کارآمد با ویروس های کامپیوتری به روزسازی مرتب این برنامه ها می باشد. ما در این قسمت دلایلی را برای به روزسازی و استفاده از نسخه های جدید ویروس یاب آورده ایم البته شما شاید بتوانید موارد دیگری را به آن اضافه کنید:

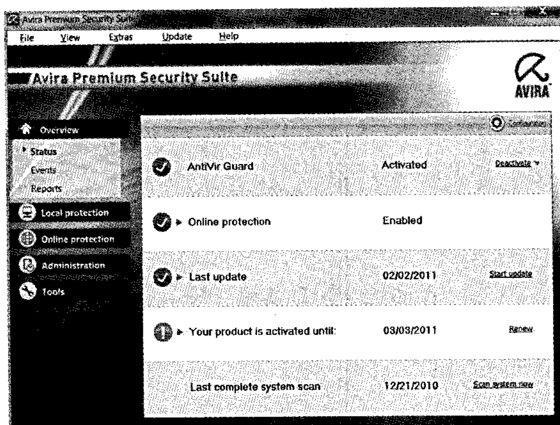
☑ با نسخه های قدیمی برنامهٔ ضد ویروس نمی توان مدت زیادی به سپر دفاعی ضد ویروس تکیه کرد.

☑ کار با نسخه های جدید ویروس یاب ها امروزه بسیار ساده تر می باشد.

☑ نسخه های جدید برنامه های ضد ویروس، دارای امکانات بیشتری می باشند.

☑ نسخه های جدید برنامه های ضد ویروس با سیستم عامل جدید و برنامه های ارسال و دریافت e-mail هماهنگی بیشتری دارد.

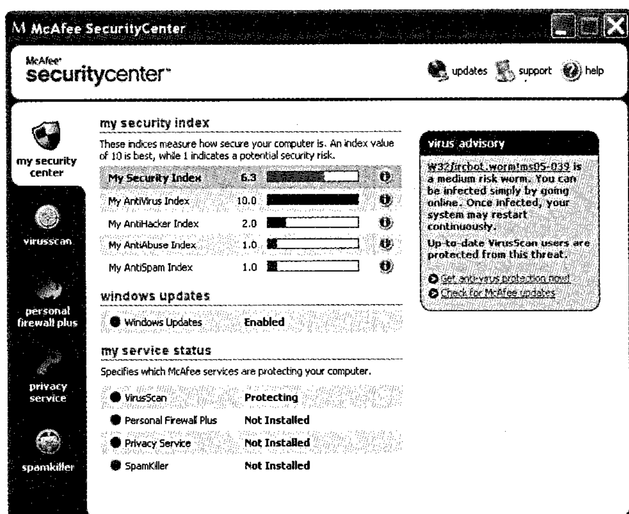
☑ نسخه های جدید برنامه های ویروس دارای محیط کاری جذاب و زیباتری هستند.



گام دوم: دلایل توجه به نوع ضد ویروس

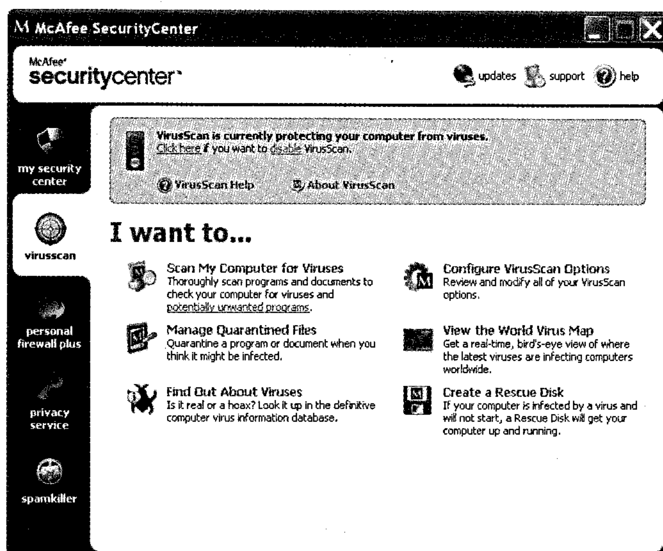
آیا شما کتاب «چه کسی پنیر مرا جابجا کرد؟» نوشتهٔ نویسندهٔ بزرگ اسپنسر جانسون را مطالعه کرده اید. در این کتاب روش های برخورد با مشکلات و تغییرات زندگی به صورت استادانه ای مطرح گردیده است. این کتاب به شما می آموزد که با عدم دلبستگی به روشهای یکنواخت زندگی و انجام تغییرات بنیادی، زندگی زیباتری را برای خود فراهم آوریم.

در دنیای ویروس ها نیز شما به استفاده دراز مدت از یک برنامهٔ ضد ویروس اصرار نداشته باشید و از تغییر برنامهٔ ضد ویروس خود نهراسید.



عادت کنید اکثر برنامه های جدید ضد ویروس را امتحان کرده و بهترین برنامه را از بین آنها انتخاب نمایید. در زیر تعدادی از دلایل منطقی برای تغییر برنامهٔ ضد ویروس مورد استفادهٔ شما گرد آمده است:

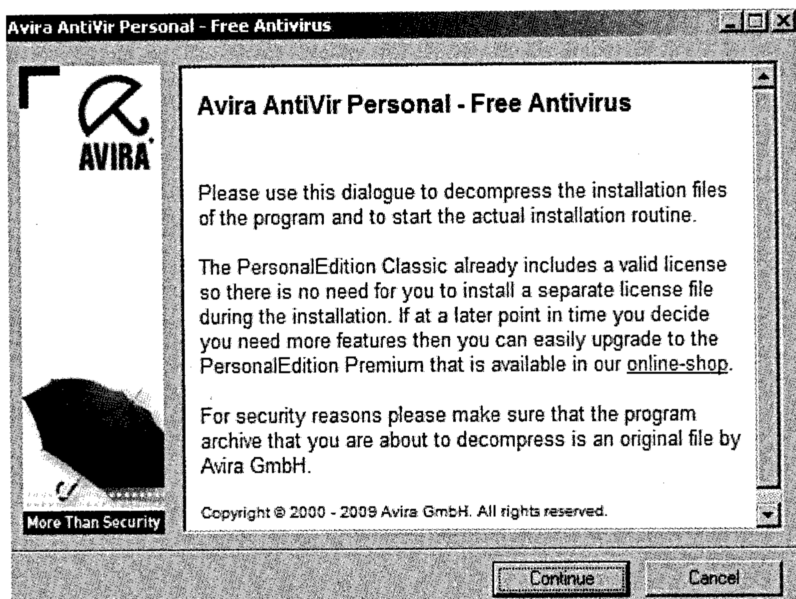
☑ عدم توانایی برنامهٔ ضد ویروس در برخورد با بعضی از ویروس ها
☑ عملکرد بهتر بعضی از برنامه های ضد ویروس در محل کار و یا محیط کار
☑ داشتن قابلیت های بالاتر و سادگی استفاده از نسخه های جدید برنامه های ضد ویروس
☑ عدم کارآیی نسخه های قدیمی ضد ویروس در محیط فعلی
☑ کارآیی فراهم نسخه های جدید برنامه های ضد ویروس



گام سوم: راهنمایی‌های قبل از نصب

قبل از هر اقدامی جهت به روزسازی و تغییر نسخهٔ برنامهٔ ضد ویروس به نکات زیر توجه داشته باشید:

☑ قبل از هر اقدامی مطالعاتی را در مورد قابلیت های نسخهٔ قدیمی و نسخهٔ جدید برنامهٔ ضد ویروس داشته باشید.
☑ از فایل های اطلاعاتی مهم حتماً پشیبان گیری کنید.
☑ هنگام نصب و یا به روزسازی برنامهٔ ضد ویروس، همهٔ برنامه های فعال را ببندید.
☑ از بهترین برنامه های ضد ویروس وترجیحاً شناخته شده استفاده کنید.



☑ قبل از هر اقدامی جهت به روزسازی یا حذف برنامه های ضد ویروس، کامپیوتر را یک بار خاموش و روشن کنید.

☑ از برنامهٔ ضد ویروس مناسب با نیازهای خود بهره بگیرید.

> **بیشتر بدانیم: سال ضرر رسانی ویروس ها**
>
> متخصصان امنیتی اعلام کردند سال ۲۰۰۴ پر هزینه ترین سال برای کاربران و شرکتها جهت مقابله با ویروس ها و هکرها بوده است. ویروس ها و هکرها در کل بیش از ۱۷/۵ میلیارد دلار به کامپیوترها و شبکه های دنیا خسارت وارد کرده اند در صورتی که در سال ۲۰۰۳ این رقم ۱۳ میلیارد دلار بوده است.

گام چهارم: نصب برنامهٔ ضد ویروس

یکی از مهمترین مراحل در فرایند استفاده و به کارگیری برنامه های ضد ویروس نصب آنها می باشد. رعایت اصول و نکات هنگام نصب به شما در استفادهٔ بهینه از ویروس یاب و قابلیت های آن کمک شایانی می کند.

قبل از هر اقدامی جهت نصب برنامهٔ ویروس یاب به نکات زیر توجه کنید:

☜ **پشتیبان گیری از فایل ها:** قبل از انجام هر اقدامی جهت نصب برنامهٔ ضد ویروس ، برای جلوگیری از حوادث غیر مترقبه حتماً از فایل های مهم کامپیوتر خود نسخه های پشتیبان تهیه کنید.

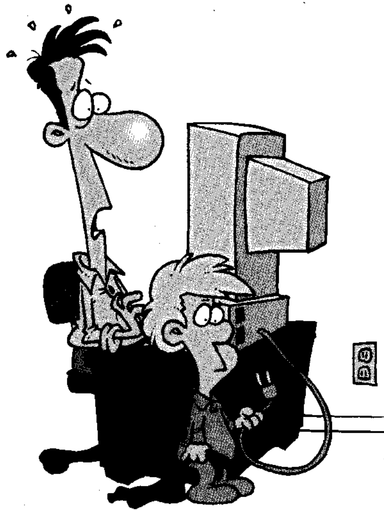
☜ **برنامه های دیگر را غیر فعال کنید:** برای نصب دقیق و سریع برنامهٔ ضد ویروس برنامه های دیگر را غیر فعال کنید.

☜ روش های مختلف نصب و به روزسازی برنامه های ویروس یاب را **بررسی** کنید.

☜ **نت برداری کنید:** محل نصب و در صورت نیاز نام کاربر از مواردی است که **یادداشت کردن** آنها ضروری می باشد.

☜ **در صورت نیاز کمک بگیرید:** از منابع مختلف جهت راهنمایی (مثل وب سایت، راهنمای برنامه) بهره بگیرید.

☜ بعد از نصب، کامپیوتر را **روشن/خاموش** کنید.



بیشتر بدانیم: خطرناک ترین اسب تروا در سال ۲۰۰۴

شرکت پاندا طی گزارشی اعلام کرد که اسب تروا **Downloader.GK** مهمترین و پرنفوذترن برنامهٔ مخرب در سال ۲۰۰۴ بوده است.

هنگامی که کاربران اینترنت از سایت های مخصوصی که برای انتشار این اسب تروا طراحی شده اند بازدید می‌کنند، پیغامی ظاهر می شود که از کاربران می خواهد برای نصب یک برنامهٔ مخصوص بر روی کامپیوتر خود اجازه دهند و اکثر آنها نیز گزینهٔ **OK** را فشار می دهند، در همین حین کامپیوتر آنها آلوده می شود.



گام پنجم: روش استاندارد نصب برنامه‌های ضدویروس

در این گام ما قصد داریم به بررسی روشی استاندارد جهت نصب برنامه های ضد ویروس بپردازیم. روشی که قابل استفاده در نصب تمام برنامه های ضد ویروس باشد، پس با ما همراه شوید:

نسخهٔ قبلی ضد ویروس را حذف کنید!

برای استفاده از حداکثر کارآیی برنامهٔ ضد ویروس جدید، بهتر است نسخهٔ قدیمی برنامه را از روی کامپیوتر خود حذف کنید. هنگام نصب برنامه های ضد ویروس جدید یکی از دو درخواست زیر را مشاهده می کنید:

☑ برنامهٔ ضد ویروس در حال نصب از شما می پرسد آیا می خواهید نسخهٔ قبلی را حفظ کنید؟ در صورت تمایل شما می توانید نسخهٔ قبلی برنامه را نگهداری کنید.

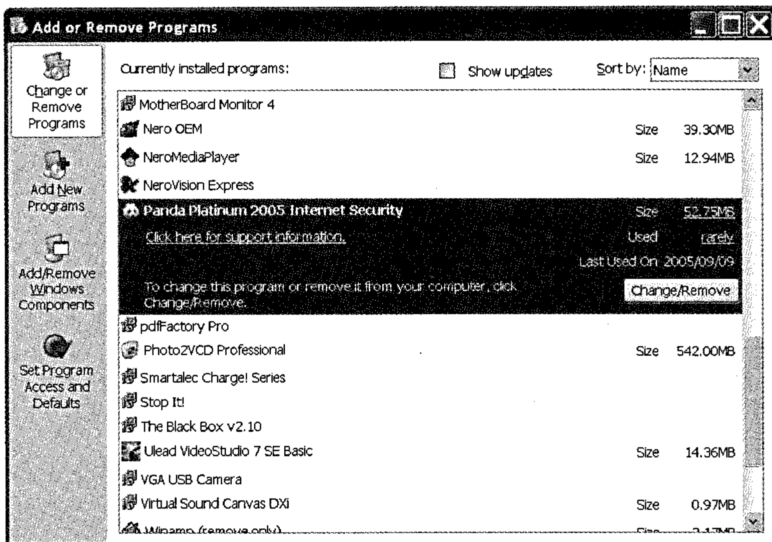
☑ برنامهٔ ضد ویروس در حال نصب از شما می خواهد نسخهٔ قدیمی ضد ویروس را حذف کنید. در این حالت جهت نصب نسخهٔ جدید باید نسخهٔ قدیمی را حذف کنید.

برای حذف نسخهٔ قبلی برنامهٔ ضد ویروس :

۱- دستورات Start→Control Panel را انتخاب کنید.

۲- در پنجرهٔ باز شده گزینهٔ Add/Remove Programs را کلیک کنید.

۳- در پنجرهٔ ظاهر شده، برنامهٔ ضد ویروس را انتخاب کرده و کلید Remove را انتخاب کنید.



برنامهٔ نصب ضد ویروس را فعال کنید!

بعد از اینکه نسخهٔ قبلی برنامهٔ ضد ویروس را از کامپیوتر خود حذف کردید حالا وقت آن رسیده که اقدام به نصب برنامه کنید. هنگام نصب برنامهٔ ضد ویروس به نکات زیر توجه کنید:

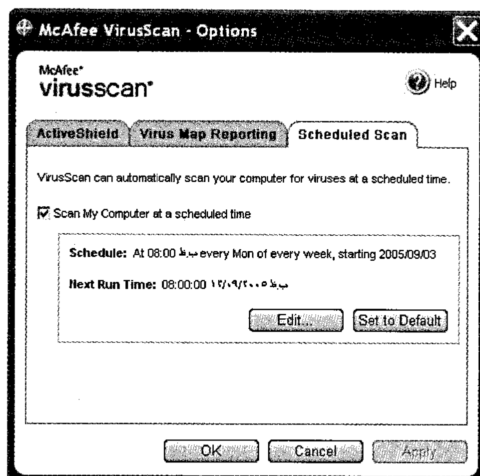
☑ **مسیر و محل نصب** برنامهٔ ویروس یاب را از قبل معین کنید.

☑ اجازه دهید آیکونی از برنامه در **کنار ساعت** کامپیوتر شما قرار گیرد.

☑ قابلیت **فعال سازی اتوماتیک** برنامهٔ ضد ویروس را فعال کنید.

☑ بعد از نصب، اجازه دهید برنامهٔ ضد ویروس تمام رسانه های قابل جابجایی شما را **بررسی** کند (مثل فلاپی دیسک، CD و ...).

☑ به قابلیت **اسکن خودکار** برنامهٔ ضد ویروس توجه خاصی را مبذول دارید.

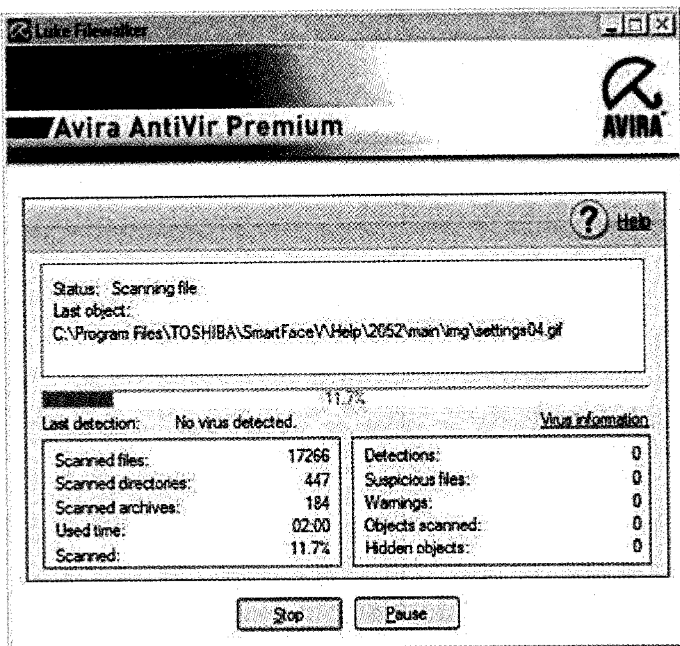


به اینترنت متصل شوید

بلافاصله بعد از نصب برنامهٔ ضد ویروس به اینترنت متصل گردیده و فایل های لازم را از وب سایت برنامه دانلود کنید. هنگام اتصال به اینترنت اکثر برنامه های ضد ویروس این کار را به صورت اتوماتیک انجام می دهند.

اسکن کامپیوتر

بعد از نصب برنامهٔ ضد ویروس کلیهٔ محتویات کامپیوتر خود را جهت ویروس زدایی اسکن کنید.



کامپیوتر خود را روشن/ خاموش کنید!

بعد از نصب برنامهٔ ضد ویروس جهت شناسایی بهتر برنامه توسط سیستم عامل، کامپیوتر را یک بار روشن/ خاموش کنید.

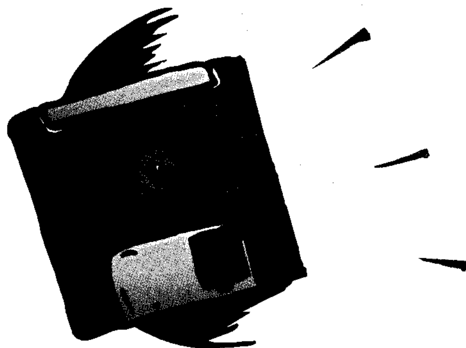
گام ششم: ساخت دیسک نجات

فرایند نصب ویروس ها را بدون ساخت دیسک نجات می توان یک فرایند نیمه کاره دانست. ولی دیسک نجات چیست؟

هنگام کار با کامپیوتر در صورتی که کامپیوتر شما در اثر حملهٔ ویروس ها نتواند فعال شود دیسک نجات به فعال سازی کامپیوتر شما کمک می کند. دیسک نجات همانطور که از اسم آن نیز مشخص است در بعضی مواقع **نجات بخش** است.

اکثر برنامه های ضد ویروس معتبر به شما امکان ساخت یک دیسک نجات را می دهند و اکثراً دارای گزینه ای به نام Create a Rescue Disk برای این منظور می باشند.

ساخت یک دیسک نجات وقت زیادی نمی گیرد و چیزی در حدود ۵ دقیقه طول می کشد ولی باور کنید که ارزش این وقت گذاشتن را دارد. برای ساخت یک دیسک نجات شما نیاز به یک فلاپی دیسک خالی دارید. بعد از ساخت دیسک نجات فراموش نکنید که **کلید قفل فلاپی دیسک** را بزنید.



خلاصهٔ این فصل

در این فصل ما با روش های کارآمد نصب و نگهداری ضد ویروس اعم از به روزسازی برنامهٔ ضد ویروس، نکات مهم قبل از نصب، نکات مهم جهت نصب ضد ویروس، روش استاندارد نصب و روش ساخت دیسک نجات آشنا شدیم. به هر یک از این موارد ذکر شده دقت کرده و به دقت آنها را بررسی کنید.

سئوالات تستی

دیسک نجات را تعریف کنید؟

الف: دیسکی برای بازیابی اطلاعات

ب: دیسکی برای فعال کردن کامپیوتر

پ: یک دیسک پشتیبانی کننده از اطلاعات

ج: همهٔ موارد صحیح است

مهمترین دلیل بروزسازی ضد ویروس چیست؟

الف: بالا بردن قدرت دفاعی ضد ویروس

ب: سادگی کار با نسخه های جدید ضد ویروس

پ: دارا بودن امکانات بهتر نسخه های جدید

ج: همهٔ موارد صحیح است

«سخنان درگوشی»

چرا دیسک‌های فشرده ۷۴ دقیقه‌ای هستند؟

دیسک‌های فشرده یا همان CD که امروزه کاربردهای فراوانی در زندگی ما دارند، در سال ۱۹۸۰ به دنیای کامپیوتر معرفی گردید. ولی چرا دیسک‌های فشرده ۷۴ دقیقه‌ای هستند نه ۶۰ دقیقه‌ای و نه ۷۰ دقیقه‌ای؟!

شرکت سونی و فیلیپس که آن زمان در حال طراحی استاندارد CD بودند بین اندازهٔ دیسک‌های فشرده با هم اختلاف داشتند. شرکت فیلیپس به دنبال طراحی دیسک‌هایی با قطر ۵/۱۱ سانتی‌متر بود و شرکت Sony به دیسک‌هایی با قطر ۱۰ سانتی‌متر بسنده کرده بود.

هر کدام از ۲ استاندارد فوق می‌توانستند ۶۰ دقیقه از موسیقی استریو با نرخ ۱۶ بیت و با فرکانس ۴۴ هرتز را در خود جای دهند.

ولی این مقدار از دید آقای نوریو اُهکا کافی نبود. وی که یک تاجر ابزار الکترونیکی در ژاپن بود و برای خوانندگی اپرا هم تعلیم دیده بود، پس از اینکه از کیفیت پایین ضبط صوت سونی شکایت کرد به استخدام آن شرکت درآمد و پس از گذشت چندسال در سال ۱۹۸۲ مدیر شرکت Sony شد. وی که علاقهٔ خاصی به موسیقی کلاسیک داشت، اصرار داشت که باید سمفونی ۹ لودویک وان بتهوون را حتماً بر روی یک CD جای داد. این سمفونی که در سال ۱۹۵۱ در شهر آلمان به مدت ۷۴ دقیقه اجرا شده بود و با اصرار نوریو ظرفیت CDها به ۷۴ دقیقه تغییر یافت.

و این بود سرآغاز CDهای ۱۲ سانتی‌متری که ۷۴ دقیقه ظرفیت داشتند، استانداردی که متأثر از نوابغ آلمانی و ژاپنی ایجاد شد.

فصل ۶

مقابله با ویروس‌ها

آیا شما هم این ضرب المثل را شنیده اید که پیشگیری همیشه بهتر از درمان است. این سخن تا حد زیادی در مورد ویروس های کامپیوتری نیز صادق است. به این معنی که در بسیاری از مواقع جلوگیری از ورود ویروس ها به کامپیوتر، به مراتب ساده تر از رفع آنها است.
روش های مختلفی برای مقابله با ویروس ها توصیه می شود که شما می توانید تا حدی ضریب امنیتی خود را در مقابل ویروس ها بالا ببرید. البته این نکته را مد نظر داشته باشید که هیچ روش صد در صدی برای مقابله با ویروس ها وجود ندارد ولی این موضوع را نمی توان دلیلی بر بی توجهی به این امر دانست.

بیشتر بدانیم: هیچ روشی صد در صد در کار نیست؟
بر اساس تحقیقات یکی از مجلات بزرگ علمی ایالات متحدهٔ آمریکا دستورات مورد نیاز و صادره کامپیوتر از یک روش منطقی واحد و معین در پردازنده ها پیروی می کنند. مثلاً بر اساس محاسبات انجام شده، در سیستم هدایت و جهت یابی موشک، ۱۰ به توان ۱۸ روش منطقی موجود است که در صورت بروز مشکل کلیهٔ این روشها جهت یافتن ویروس باید بررسی شوند. تا اینجا هیچ مشکلی نیست، ولی مسئلهٔ اساسی این است که اگر هر آزمایش و تست در زمانی معادل یک میکرو ثانیه طول بکشد شما باید عمری به درازای ۳۲۰۰۰ سال داشته باشید.

گام اول: روش‌های کلّی مبارزه با ویروس‌ها

همانطور که گفته شد جلوگیری از ورود ویروس های کامپیوتری به سیستم، ساده تر از دفع آنها می‌باشد. به طور کلی روش های اصلی مبارزه با ویروس را می توان به سه دسته تقسیم کرد:

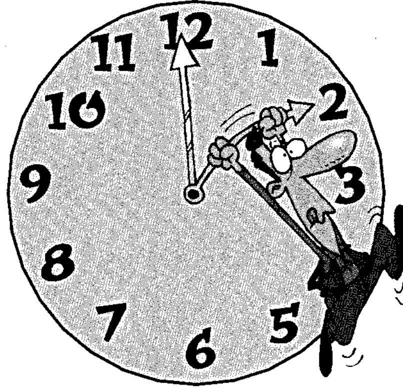
۱- جلوگیری از ورود ویروس ها به سیستم برای محدود کردن انتشار و شیوع آنها
۲- پی گیری و شناسایی ویروس جهت بالا بردن قدرت تدافعی کامپیوتر
۳- از بین بردن ویروس های وارد شده به سیستم و بازگرداندن وضعیت سیستم به حالت عادی



هر روزه ویروس های جدید با سرعت خیره کننده ای به وسیلهٔ ویروس نویسان به دنیای کامپیوتر هدیه می شوند و چه بسا تا شناخت این ویروس ها و تهیهٔ برنامهٔ ضد ویروس، هزاران کامپیوتر در معرض حمله و تخریب این ویروس ها قرار می گیرند. از طرفی شرکت های تولید کنندهٔ برنامه های ضد ویروس با دریافت ویروس های جدید و برنامهٔ ضد ویروس آن می توانند برنامه ای مناسب را جهت مقابله با آنها ارایه دهند.
بنابراین یکی از مؤثرترین روش ها جهت مقابله با ویروس ها را می توان پیروی از اصولی به شرح زیر دانست:

پشتیبان گیری از اطلاعات کامپیوتر

یکی از مهمترین اقدام جهت مقابله با هر گونه تخریب اطلاعات را می توان گرفتن نسخه های پشتیبان بر اساس یک برنامهٔ مدون و قابل اجرا دانست. مداومت و نظم در فرایند پشتیبان گیری اطلاعات یکی از اصول مهم و حیاتی در جهت حفظ اطلاعات می باشد. از طرفی نگهداری و حفظ این نسخه های پشتیبان را نیز می توان عامل مهم در بازیابی اطلاعات در زمان مناسب دانست.
تنظیم زمان بندی تهیهٔ نسخه های پشتیبان از اطلاعات به عوامل مختلفی مثل حجم اطلاعات ذخیره شده، نوع اطلاعات و ارزش آنها بستگی دارد.



☺ همراه: در صورت استفاده از فلاپی دیسک جهت گرفتن پشتیبان حداکثر سعی نمایید که آنها را بعد از ضبط اطلاعات در حالت Write Protect قرار دهید.

برنامهٔ ضد ویروس مطمئن

یکی از نکات مهمی که در مقابله با ویروس های کامپیوتری در کشور ما متأسفانه به آن توجه نمی‌شود عدم استفاده از یک برنامهٔ ضد ویروس مطمئن و معتبر می باشد. تأکید ما این است که شما حدالامکان سعی کنید که برنامه ضد ویروس خود را از یک منبع مطمئن، قابل اعتماد و خوشنام تهیه کنید.

هنگام خرید برنامهٔ ضد ویروس از سالم بودن بسته بندی نرم افزاری و غیر کپی و معتبر بودن آن اطمینان حاصل کنید. زیرا ممکن است یک کپی غیر مجاز، خود عامل آلودگی ویروسی کامپیوتر شما باشد.

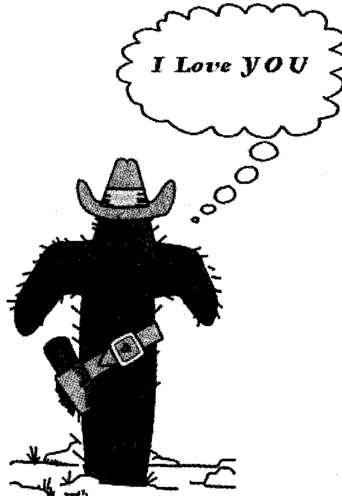


از بین بردن اسپم ها یا E-mail های ناخواسته

همانطور که قبلاً نیز به آن اشاره شده یکی از مشکلات اکثر کاربران اینترنتی هنگام بررسی صندوق پست الکترونیکی خود، برخورد مهمان های ناخوانده ای به نام اسپم ها می باشد.

امروزه بسیاری از کرم ها و ویروس های کامپیوتری خود را از طریق این نامه های الکترونیکی منتشر می کنند. متن و عنوان اسپم ها به صورتی انتخاب می شود که هر بیننده ای با دیدن آن هوس می کند که آن را باز کند. غافل از اینکه پس از باز کردن E-mail یک نفر به قربانیّان ویروس ها اضافه می شود.

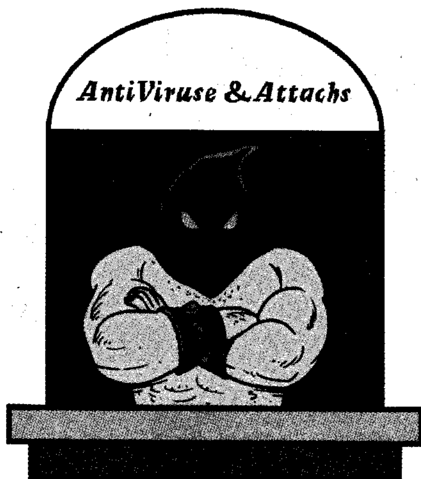
بنابراین بصورت اکید توصیه می شود که از مطالعه و خواندن E-mail های ناشناس با عناوین تحریک کننده ای مثل I Love You خودداری کرده و در اولین فرصت آنها را از بین ببرید.



استفاده از برنامهٔ ضد ویروس و پیوست های امنیتی

استفاده از برنامه های ضد ویروس، برنامه های امنیتی و فعال کردن گارد آنها بر روی سیستم، معمولاً از ورود ویروس های کامپیوتری تا حد زیادی جلوگیری می کند و احتمال آلوده شدن به ویروس ها را به طور چشمگیری کاهش می دهد.

هنگام استفاده از برنامه های ضد ویروس و **پیوست های امنیتی** آنها حدالامکان سعی کنید اطلاعات این برنامه ها برای مقابلهٔ هر چه بهتر با ویروس ها همیشه به روز باشد.



گام دوم: راه کارهای دقیق برای مقابله با ویروس‌ها

در گام قبل ما با روش های کلی مبارزه با ویروس ها آشنا شدیم. در این گام قصد داریم با ارائهٔ راه کارهایی دقیق، احتمال آلودگی کامپیوترهای خود را به حداقل برسانیم.

مهمترین گام جهت مقابله با ویروس ها در سطح یک شرکت و گروه استفاده کننده از کامپیوتر، وضع قوانین مدون و قابل اجرا می باشد. این مقررات باید کاملاً قابل اجرا بوده و ضمانت اجرایی کافی داشته باشد. به هر حال در این قسمت پیشنهاداتی را برای جلوگیری از ورود ویروس ها گرد آورده‌ایم که امید است مفید واقع شود.

جلوگیری از نصب برنامه ها

از نصب هر گونه برنامه ای به وسیلهٔ کاربران بر روی کامپیوتر و کامپیوترهای مدیریت جلوگیری کنید. سیستم تحت مدیریت خود را به صورتی تنظیم کنید که هرگونه نصب برنامه از طریق کانال کنترل مدیریتی شما انجام گردد. از تست و آزمایش برنامه های ناشناخته بر روی کامپیوتر، خودداری کنید.



حافظت از فایل های اجرایی

از فایل های مهم و اجرایی کامپیوتر خود به دقت مراقبت کنید. بر اساس یک برنامۀ مدون، تغییرات احتمالی در نام یا حجم فایل های اجرایی و اطلاعاتی مهم را بررسی کنید.



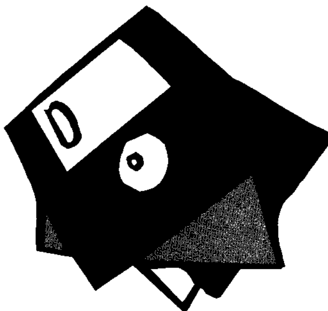
نظارت بر فایل های رد و بدل شده

هنگام دریافت و ارسال فایل های اطلاعاتی بر نوع و ساختار فایل ها دقت کافی را مبذول دارید. هنگام انتقال اطلاعات دقت داشته باشید که فایل ها حاوی هیچگونه فایل اجرایی نباشند. به دلیل اینکه فایل های اجرایی پناهگاهی مطمئن برای ویروس ها می باشند.



از دیسک Boot جهت فعال سازی استفاده کنید!

برای فعال سازی کامپیوتر خود حدالامکان سعی کنید از دیسک های Boot جهت فعال سازی کامپیوتر استفاده نکنید. بر اساس تحقیقات انجام شده این فلاپی های Boot می تواند عاملی مهم برای ویروسی شدن کامپیوتر شما باشد.



استفاده از کلمهٔ رمز مناسب

با استفاده از کلمهٔ رمز مناسب از دسترسی غیر مجاز افراد دیگر جهت دستیابی به اطلاعات کامپیوتر خود جلوگیری کنید. برای تعریف یک کلمهٔ رمز به توصیه های زیر توجه کنید:

☑ از حروف بزرگ و کوچک در کلمهٔ رمز به صورت یکی در میان استفاده کنید (AbCnM).

☑ از نام خانوادگی، تاریخ تولد و عناوینی مشخص استفاده نکنید.

☑ هر سه ماه یک دفعه کلمهٔ رمز خود را تغییر دهید.

☑ کلمهٔ رمز خود را در هیچ جایی یادداشت نکنید و آنرا در اختیار هیچ کس قرار ندهید و ...

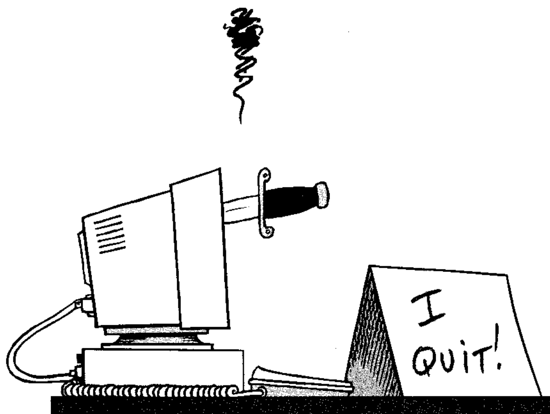


ضد ویروس محلی

حتماً از یک برنامهٔ ضد ویروس شناخته شده و ترجیحاً محلی (ملّی) که تمام ویروس های رایج کشور شما را می شناسد استفاده کنید. چه بسا ضد ویروس های خوبی که در سطح بین المللی بسیار پرقدرت هستند ولی در مقابله با ویروس های محلی یک کشور بسیار عاجز می باشند.

کامپیوتر را یک بار خاموش/ روشن کنید

در صورتی که کامپیوتر شما به صورت اشتراکی مورد استفاده قرار می گیرد قبل از شروع به کار کامپیوتر را یکبار خاموش/ روشن کنید. تعدادی از ویروس ها با پنهان شدن در حافظهٔ RAM اقدام به عملیات تخریبی می کنند. شما با **خاموش/ روشن کردن** کامپیوتر می توانید این ویروس ها را از بین ببرید.



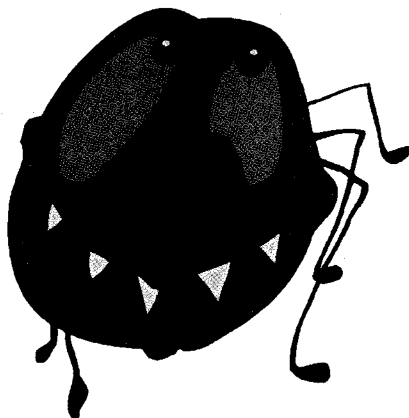
فعال سازی مداوم برنامهٔ ضد ویروس

هیچگاه برنامهٔ ضد ویروس را در کامپیوتر خود یا کامپیوترهای تحت شبکه غیر فعال نسازید. یک ویروس برای آلوده سازی کامپیوتر شما به زمان زیادی نیاز ندارد.

ترس برادر مرگ است!

همهٔ اتفاقات ناگوار کامپیوتری ناشی از عملکرد ویروس ها نیست و خیلی از عملکردهای نادرست سیستم های کامپیوتری را می توان ناشی از اختلالات سخت افزاری یا نرم افزاری و **عدم مهارت کاربر** دانست.

بسیار اتفاق افتاده که با ترس بی مورد کاربران از ویروس ها به فایل های اطلاعاتی کامپیوتر خسارات جبران ناپذیری وارد شده است.



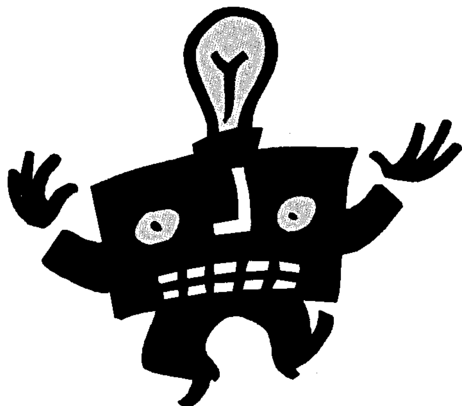
دانلود اطلاعات در اینترنت

ویروس های زیادی در دنیای اینترنت، در قالب برنامه های رایگان قابل دانلود وجود دارند. رایگان بودن اکثر این برنامه ها مهمترین انگیزهٔ دانلود آنها می باشد. بنابراین به دانلود این برنامه و فایل‌های اطلاعاتی موجود در اینترنت بسیار دقت کنید.

اتفاق خبر نمی کند!

افراد زیادی هستند که ادعا می کنند بعد از سالها کار کردن با اینترنت و کامپیوتر هرگز به هیچ ویروسی برخود نکرده اند. ویروسی شدن کامپیوتر تنها **در یک لحظه اتفاق** می افتد، لحظه ای که شما هیچ وقت انتظار آن را نداشته اید.

ویروسی شدن، یک فرایند غیر قابل اجتناب در دنیای کامپیوتر و اینترنت می باشد پس نکته های ایمنی جهت مقابله با آنها را جدی بگیرید.



خلاصهٔ این فصل

در این فصل روش هایی را برای مقابله با ویروس ها بررسی کردیم. به کارگیری هر کدام از این روش ها مانعی در مقابل ویروس ها می باشد و شانس آلوده نشدن سیستم شما را تا حد زیادی بالا می برد. بسیاری از این روش های مقابله، بسیار ساده می باشد که عدم توجه به آنها خسارات جبران ناپذیری را به بار می آورد. پیام اصلی این فصل را می توان در یک سطر خلاصه کرد **«ویروس ها را جدی بگیرید»**.

سئوالات تستی

چرا در فایل های رد و بدل شده بین کامپیوتر خود و دیگر کامپیوترها به فایل های اجرایی باید بیشتر توجه کرد؟

الف: چون این فایل ها دارای اهمیت بیشتری می باشند

ب: چون این فایل ها پناهگاهی مطمئن برای ویروس ها می باشند

پ: چون این فایل ها بسادگی انتقال می یابند

ج: گزینهٔ الف و پ

نکات مهم در تعریف و انتخاب یک کلمهٔ رمز را بنویسید؟

الف: استفاده از حروف بزرگ و کوچک

ب: استفاده نکردن از موضوعات مشخص



پ: تغییر مداوم ضد ویروس

ج: همهٔ موارد صحیح است

استفاده از یک برنامهٔ ضد ویروس معتبر (یا به اصطلاح غیر کپی) چه تأثیری در عملکرد بهتر آن دارد؟

الف: محیط کاری مطمئن تری را برای ما فراهم می کند

ب: به روزسازی آنی به وسیلهٔ شرکت سازنده به سادگی امکان پذیر است

پ: از خدمات پشتیبانی شرکت سازنده می توان بهره برد

ج: هیچکدام

«سخنان درگوشی»

شیوهٔ کار یک هکر برای دست‌یابی به کلمهٔ رمز و نام کاربری شما چگونه است؟!

شما احتمالاً از یک رمز مشترک برای اکانت‌های زیادی استفاده می‌کنید! آیا این طور نیست؟ برخی از وب‌سایت‌ها مثل سایت بانکی‌تان و یا VPN اتصال به ادارهٔ تان، معمولاً از امنیت قابل قبولی برخوردار هستند. پس هکرهای حرفه‌ای مثل من اصلاً وقت خود را برای آن تلف نمی‌کنند. من برای شروع به وب‌سایت‌هایی (مثل سایت‌های کارت تبریک) که شما همیشه به آنها مراجعه می‌کنید سری می‌زنم. علاوه بر این از برنامه‌های حدس زدن رمز عبور مثل Brutus و Thc استفاده می‌کنم.
علاوه بر این با استفاده از شیرینی‌های کوچک و خوشمزه‌ای به نام کوکی‌ها به سادگی می‌توانم حدس بزنم که شما در کدام بانک حساب دارید و نام کاربری‌تان چیست؟
حال شاید بپرسید این فرایند چقدر وقت می‌گیرد؟!
این مدت زمان به عوامل مختلفی مثل نوع رمز و سختی آن و دوم سرعت عملکرد هکر و سوم سرعت خط اینترنت هکر بستگی دارد. پس همین‌طور که متوجه شدید در حفظ کلمهٔ رمز پیچیدگی آن کارت برندهٔ شما است. اما این واقعیتی است که به خاطر سپاردن کلمات عبور طولانی نیز بسیار مشکل و آزار دهنده است. پس توصیه می‌کنیم: هنگام تعریف کلمهٔ رمز از حروف هم قیافه مثل صفر (۰) و O (اُ) و یا @ به جای a استفاده کنید. از ابتدای اسامی مختلف مثل مکان مورد علاقه یا گل مورد نظرتان بهره ببرید. در نهایت پس از انتخاب کلمهٔ رمز با استفاده از سرویس‌هایی مثل Password Strengh test مایکروسافت میزان امنیت آنرا آزمایش کنید. نکتهٔ آخر اینکه همهٔ رمزها و کلمات عبور خود را مهم بدانید و از یک سطح امنیتی بالا برای همهٔ آنها بهره ببرید.

فصل ۷

انتخاب بهترین برنامهٔ ضد ویروس

در دنیای کامپیوتر ما هر روز شاهد تولد برنامه های جدید ضد ویروس هستیم که هر کدام ادعا دارند که به بهترین نحو ممکن کامپیوتر شما را از شر ویروس ها نجات می دهند.
آیا شما داستان علاء الدین و چراغ جادو را خوانده اید؟ دراین داستان علاء الدین به وسیلهٔ غول چراغ جادو به هر آرزویی که دوست داشت دست پیدا می کرد. اکثر برنامه های جدید ضد ویروس نیز ادعا دارند که بصورت کاملاً جادویی کامپیوتر شما را در مقابل ویروس ها بیمه می کنند.
ولی متأسفانه ما در دنیای برنامه های ضد ویروس، هیچ چراغ جادویی را نداریم (ولی ای کاش داشتیم). هیچکدام از این برنامه ها به صورت تمام و کمال نمی توانند تمام ویروس ها را از بین ببرند و کامپیوتر شما را در مقابل این خطرات محافظت کنند.
با تمام این تفاصیل استفاده از برنامه های ضد ویروس یکی از توصیه های مهم جهت جلوگیری از گسترش ویروس ها به شمار می آید. برنامه های ضد ویروس تا حد زیادی کامپیوتر شما را در مقابل ویروس ها **واکسینه** می کنند.

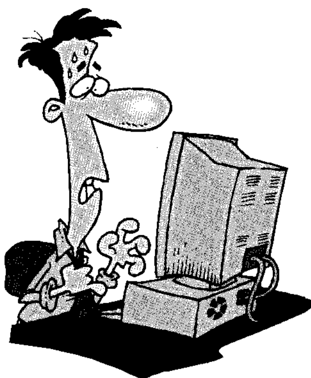
گام اول: تقسیم‌بندی برنامه‌های ضد ویروس

هنگام صحبت کردن در مورد برنامه های ضد ویروس، یکی از نکات مهمی که باید به آن توجه زیادی را داشته باشیم عملکرد واقعی هر کدام از این برنامه ها می باشد. انجمن تولید کنندگان

برنامه‌های ضد ویروس، نرم افزارهای ضد ویروس را به سه گروه مختلف تقسیم کرده است که در این گام به هر یک از آنها می پردازیم.

برنامه های ضد ویروس کلاس الف

این گروه از برنامه های ضد ویروس به صورتی طراحی شده اند تا از تکثیر و آلوده سازی اولیه به وسیلهٔ ویروس ها جلوگیری کرده و مانع از تغییر فایل های اطلاعاتی می گردند.
این برنامه ها به شما امکان می دهند تا به صورت کاملاً تنظیم شده از دستکاری فایل های خاص در کامپیوترتان جلوگیری کنید. عیب بزرگ این کلاس از برنامه های ضد ویروس را می توان **مداخلهٔ بیش از حد** در کارهای عادی شما دانست.



برنامه های ضد ویروس کلاس ب

گروه دوم برنامه های ضد ویروس به شکلی طراحی شده اند تا آلودگی های ناشی از ویروس ها را کشف کرده و اعمال مختلفی چون: محاسبهٔ مجموعه بایت های یک برنامه، بررسی مجوزها و مقایسهٔ آن با کدهای ذخیره شدهٔ قبلی را انجام می دهند.
گونه ای از این برنامه های ضد ویروس با بررسی تاریخ فایل ها، هرگونه تغییر در فایل های اطلاعاتی را کنترل می کنند. از دیگر وظایف این گروه از ضد ویروس ها کنترل پیغام های ویروس هایی است که هدف آنها تخریب روانی کاربران می باشد، پیغام هایی مثل:

«شرمنده هارد شما حالا به یک آشغال تبدیل شده است»

ویژگی منحصر به فرد این گروه از برنامه های ضد ویروس، کنترل ومحافظت از قسمت های آسیب پذیر کامپیوتر می باشد.



SYSTEN ERROR HE HE HE OH!

☺ همراه: نمی دانم شما تا به حال با این پیغام های آزار دهنده روحی برخورد کرده اید. پیغام هایی مثل «متأسفم کامپیوتر شما به یک آکواریوم تبدیل شده است». این پیغام ها در پی یک فرایند آسیب رسانی ویروسی در روی صفحهٔ نمایش ظاهر می شود بنابر این تأثیر روانی بسیار بدی بر روی کابران می گذارد در این مواقع بهتر است یک فنجان چای بخورید و در جلوی آینه کمی به خودتان دلداری بدهید.

برنامه های ضد ویروس کلاس پ

این گروه از برنامه های ضد ویروس دارای کلاس بالاتری نسبت به دیگر برنامه های ضد ویروس می باشند. این برنامه ها توسط مطابقت دادن ویروس با اطلاعات بانک اطلاعاتی خود آنها را شناسایی کرده و متعاقباً از بین می برند.

از معایب بزرگ این گروه از برنامه های ضد ویروس می توان به **عدم کارآیی آنها در مقابل ویروس های جدید** اشاره کرد. به همین دلیل به صورت مدام باید این برنامه ها را به روزسازی کرد.

از مزایای بزرگ این دسته از برنامه های ضد ویروس جای گیری در حافظه و نظارت کامل بر عملکرد سیستم می باشد. مثلاً هنگامی که در سیستم یک اتفاق یا دستورالعمل غیر معمول اتفاق بیافتد این برنامه سریع از شما به وسیلهٔ کادرهای محاوره ای کسب تکلیف می کند.



بیشتر بدانیم: جالب و شنیدنی!

بسیاری از واقعیات اطراف ما روزی تنها یک خیال و تصور بوده است. مثلاً ژول ورن در داستان های خود بعضی از واقعیات فعلی زندگی مان را مثل سفر به ماه، دور دنیا در ۸۰ روز و ... را به صورت خیالی درج کرده است. ولی حالا این موارد سفر به ماه و سفر به دور دنیا در عرض چند روز یک امری کاملاً طبیعی به نظر می رسد.

نمی خواهیم دل شما را خالی کنیم یا ادای ژول ورن را دربیاوریم ولی تصور کنید اگر روزی بتوان به وسیلهٔ کامپیوتر، ویروس های بیماری زا را همانند ویروس های کامپیوتری انتقال داد چه اتفاقی می افتاد.

داستان این طوری می شود که شما در یک صبح زیبای بهاری ایمیلی با عنوان **Just for You** را باز می کنید و ویروس جنون گاوی به بدن شما سرایت می کند. حتی تصور این موضوع نیز مو را به تن آدم سیخ می کند وای ...

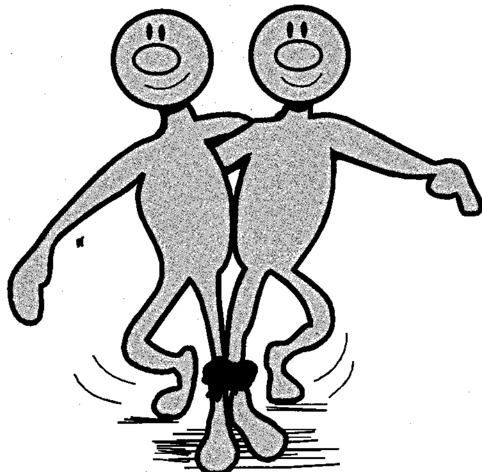
گام دوم: پارامترهای مهم در انتخاب یک برنامهٔ ضد ویروس

امیدواریم تا اینجای کتاب توانسته باشیم شما را راضی کنیم تا یک برنامهٔ ضد ویروس معتبر تهیه کرده و آنرا بر روی کامپیوتر خود نصب کنید. همانطور که قبلاً نیز به آن اشاره شده برنامه های ضد ویروس فراوانی در بازار کامپیوتر وجود دارد ولی باور کنید که تنها یکی از این برنامه ها واقعاً نیاز شما را مرتفع می کند. در این گام ما با طرح مجموعه سئوالاتی قصد داریم به انتخاب مناسب شما کمک کرده و به نگاه جستجوگرانهٔ شما جهت مثبت بخشیم. قبل از انتخاب دقیق یک برنامهٔ ضد ویروس این سئوالات را در ذهن خود مرور کنید:

✓ آیا برنامهٔ ضد ویروس انتخابی من با سیستم عامل کامپیوترم **سازگاری** دارد؟

✓ آیا برنامهٔ ضد ویروس **تداخلی** در دیگر برنامه های کاربردی کامپیوتر (مثل برنامه های حسابداری یا گرافیکی) ایجاد نمی کند؟

✓ آیا این برنامهٔ ضد ویروس در **سرعت کامپیوتر** و برنامه های کاربردی تأثیر منفی نمی گذارد؟



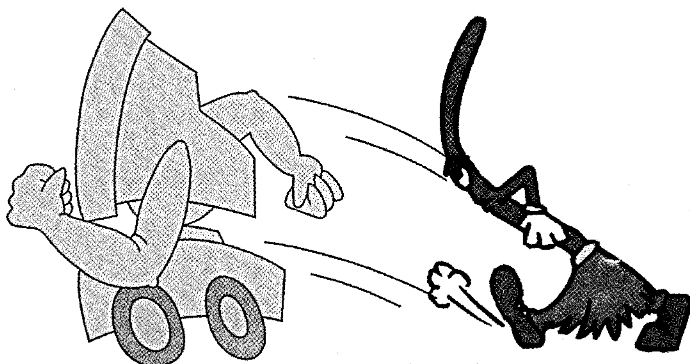
✓ آیا برنامهٔ فوق در عملکرد کاری شما ایجاد **وقفه** نمی کند؟

✓ آیا برنامهٔ فوق **قابلیت شناسایی** ویروس های محلی (و نسخه های مختلف) آنها را دارد؟

✓ آیا این برنامهٔ ضد ویروس **کاملاً معتبر** بوده و دارای خدمات پشتیبانی می باشد؟

✓ آیا این برنامهٔ ضد ویروس، **برنامهٔ خوشنامی** است؟

✓ آیا این برنامهٔ ضد ویروس آنقدر **قابل اعتماد** است که بتوان اطلاعات مهم کامپیوتر یک سازمان (مثل بانک ها) را به آن سپرد؟



این سئوالات را با خود تکرار کرده و هنگام انتخاب یک برنامهٔ ضد ویروس (قبل از خرید آن) به جواب های مناسبی دست پیدا کنید.

بیشتر بدانیم: از شایعات ویروسی جداً خودداری کنید!

در صورتی که یک برنامه نویس خبره و یا مدیر شرکت نرم افزاری هستید برنامه های تولیدی خود را قبل از ارائه به دقت بررسی کنید. وجود یک ویروس و حتی شایعهٔ وجود آن خسارات جبران ناپذیری را به اعتبار برنامه های نرم افزاری وارد می کند.

برای مثال در سال ۱۹۸۸ قرار گرفتن یک ویروس تقریباً بی خطر که حاوی پیغام صلح بود (این پیغام در دوم مارس ۱۹۸۸ در روی صفحهٔ نمایش ظاهر شد و خود به خود حذف گردید) همراه با برنامهٔ گرافیکی Freehand خسارات فراوانی را به شرکت مایکرومدیا تولید کنندهٔ این برنامه وارد کرد.

خلاصهٔ این فصل

در این فصل با یک ذره بین در دست به بررسی عوامل مؤثر جهت انتخاب بهترین برنامهٔ ضد ویروس پرداختیم. ما در این فصل با تقسیم بندی برنامه های ضد ویروس از نظر عملکرد، مزایا و معایب هر یک از آنها را مطالعه کردیم و در پایان با ذکر مجموعه سئوالاتی به انتخاب بهترین برنامهٔ ضد ویروس ممکن سرعت بخشیدیم. در فصلی که ما با هم داشتیم بالاخره به داشتن یک برنامهٔ کارآمد ضد ویروس ایمان پیدا کردیم.

سئوالات تستی

مهمترین عیب برنامه های ضد ویروس کلاس ب را بنویسید؟

الف: بالا بودن قیمت آنها

ب: بالا بودن حجم آنها

پ: پایین بودن قدرت تدافعی در مقابل هکرها

ج: عدم کارآیی در مقابل ویروس های جدید

بزرگترین مزیت برنامه های ضد ویروس کلاس ب چیست؟

الف: بالا بودن قدرت تدافعی

ب: شناسایی ویروس های جدید

پ: پایین بودن قیمت

ج: جای گیری در حافظه و نظارت کامل بر عملکرد سیستم

فصل ۸

معرفی چند برنامهٔ ضد ویروس مهم

هنگامی که جهت خرید یک برنامهٔ ضد ویروس به یکی از مراکز خرید و فروش مراجعه می کنید با یک دوجین از این برنامه ها روبرو می شوید.
در فصل قبل ما نگاهی دقیق به روش های انتخاب یک برنامهٔ ضد ویروس داشتیم. دراین فصل ما قصد داریم به بررسی خصوصیات و ویژگی های مهم معروف ترین برنامه های ضد ویروس بپردازیم.
ما در این فصل بیشتر سعی کرده ایم که ویژگی های مختلف برنامه های معروف ضد ویروس را بر اساس یک جدول ویژگی های تدوین شده، بررسی و با یکدیگر مقایسه کنیم. شما می توانید در صورت تمایل ویژگی های بیشتری را به این جدول اضافه کنید.

برنامهٔ ضد ویروس *eTrust EZ Armor*

این برنامهٔ ضد ویروس، محصولی کارآمد از شرکت Associate برای استفادهٔ تجار و بازرگانان می‌باشد، ولی می توان از آن در منزل نیز استفاده کرد. در وب سایت این شرکت می توانید هر سئوالی را که می خواهید در مورد ویروس ها و برنامه های ضد ویروس بپرسید. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:

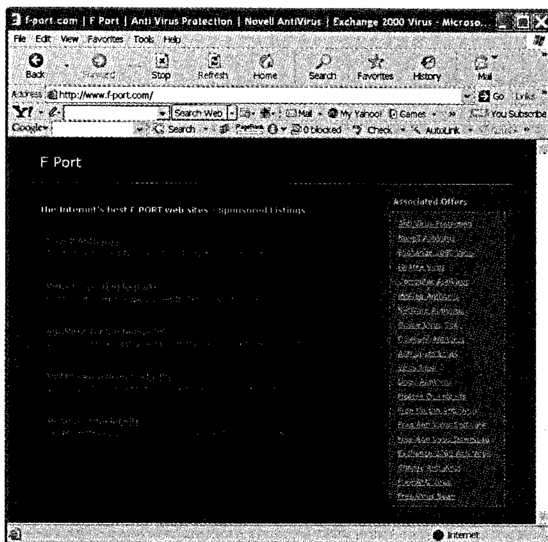




شرکت سازنده	COMPUTER ASSOCIATES INTERNATIONAL
آدرس شرکت	Islandi, NY, USA
آدرس وب سایت	www.my-etrust.com
آیا امکان تست رایگان وجود دارد؟	بله، شما می توانید ۱۲ ماه به صورت رایگان از این ضد ویروس با مراجعه به سایت www.my-etrust.com استفاده کنید.
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	خیر
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندۀ اسپم ها	خیر
بلوکه کنندۀ تبلیغات	خیر

برنامهٔ ضد ویروس *F-Port for Windows*

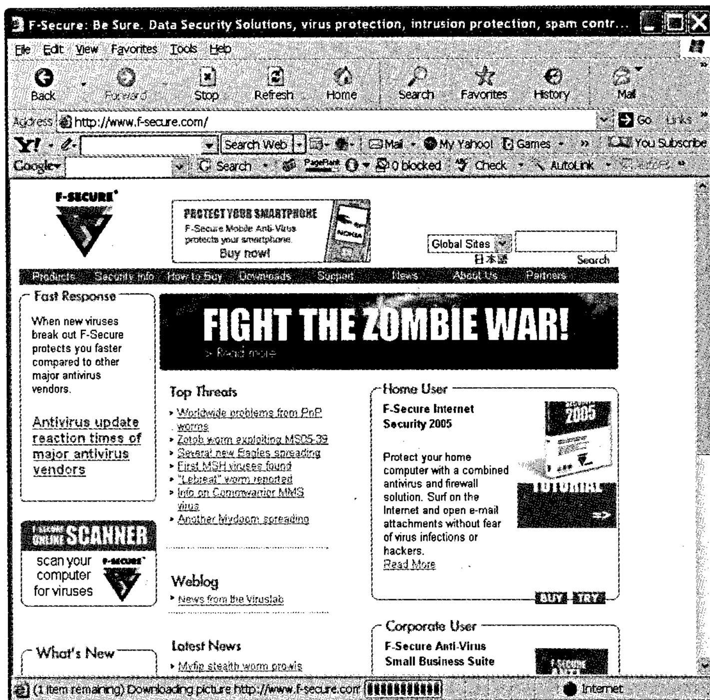
این برنامهٔ ضد ویروس در **انواع مختلفی** برای سیستم های عامل ویندوز، Dos و یونیکس از طرف شرکت Frisk ارائه شده است. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:



شرکت سازنده	FIRSK SOFTWARE INTERNATIONAL
آدرس شرکت	Reyjavik- Iceland
آدرس وب سایت	www.f-port.com
آیا امکان تست رایگان وجود دارد؟	بله، به مدت ۳۰ روز
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	خیر
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	خیر
بلوکه کنندهٔ اسپم ها	خیر
بلوکه کنندهٔ تبلیغات	خیر

برنامهٔ ضد ویروس *F-Secure*

برنامهٔ ضد ویروس F-Secure امکانات و راهنمایی های مفیدی را از طریق وب سایت خود به کاربران ارائه می دهد. این برنامه به **زبان های** انگلیسی، فرانسوی، فنلاندی، سوئدی، آلمانی و حتی ایتالیایی ارائه شده است. جدول ویژگیهای این برنامهٔ ضد ویروس به شرح زیر است:

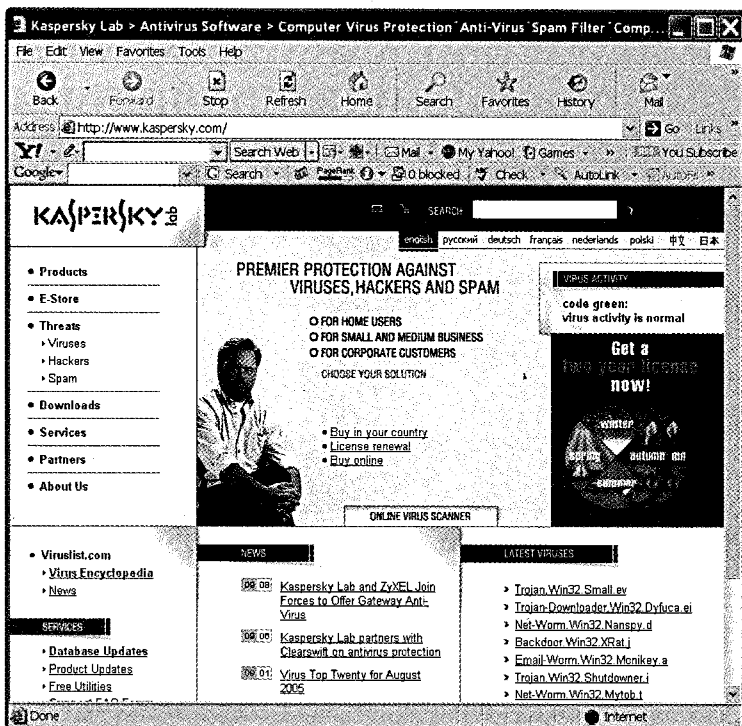


F-SECURE CORPORATION	شرکت سازنده
هلسینکی-فنلاند	آدرس شرکت
www.f-secure.com	آدرس وب سایت
بله، به مدت ۶ ماه از طریق وب سایت www.f-secure.com/protectyourpc و ۳۰ روز از طریق وب سایت www.f-secure.com/download-purchase	آیا امکان تست رایگان وجود دارد؟
بله	آیا امکان خرید Online وجود دارد؟
بله	آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟
بله	آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟

بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندهٔ اسپم ها	خیر
بلوکه کنندهٔ تبلیغات	خیر

برنامهٔ ضد ویروس *Kaspersky*

یکی از برنامه های جالب ضد ویروس که **توانایی فراوانی** در شناسایی و از بین بردن ویروس را دارا می باشد برنامهٔ Kaspersky می باشد. این برنامه محصولی از شرکت Kaspersky Labs بوده و به زبان های انگلیسی، فرانسوی، آلمانی، ایتالیایی و اسپانیایی قابل دسترس است.



شرکت سازنده	KASPERSKY LABS
آدرس شرکت	مسکو–روسیه
آدرس وب سایت	www.kaspersky.com
آیا امکان تست رایگان وجود دارد؟	بله، ۳۰ روز

سؤال	پاسخ
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله، از طریق مراجعه به وب سایت www.kaspersky.com/scanforvirus.html
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله (البته این قابلیت در قالب محصولی جداگانه ارائه شده است)
بلوکه کنندهٔ اسپم ها	خیر
بلوکه کنندهٔ تبلیغات	خیر

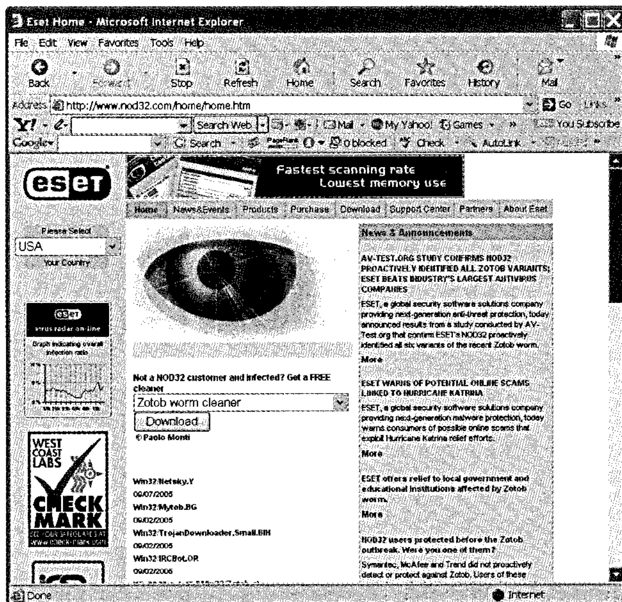
برنامهٔ ضد ویروس *McAfee*

یکی از قوی ترین برنامه های ضد ویروس دنیا، برنامهٔ McAfee می باشد. این برنامهٔ قدرتمند به زبان های انگلیسی، فرانسوی، آلمانی، ایتالیایی و اسپانیایی قابل دسترس می باشد. برنامهٔ ضد ویروس McAfee قابل استفاده در کامپیوترهای **خانگی** و **شبکه های بزرگ** کامپیوتری است. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:

شرکت سازنده	NETWORK ASSOCIATES
آدرس شرکت	Santa Clara, CA, USA
آدرس وب سایت	www.McAfee.com
آیا امکان تست رایگان وجود دارد؟	بله، ۱۵ تا ۳۰ روز از طریق سایت http://download.mcafee.com/
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندهٔ اسپم ها	بله
بلوکه کنندهٔ تبلیغات	بله

برنامهٔ ضد ویروس *NOD32*

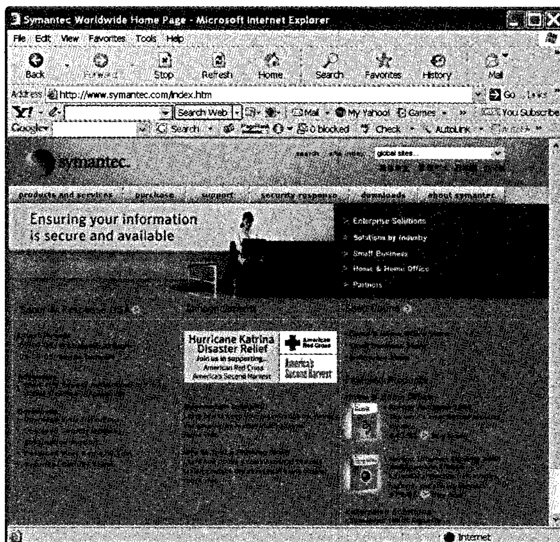
یکی دیگر از برنامه های ضد ویروس ساخت شرکت Eset Software برنامهٔ NOD32 می باشد. این برنامهٔ ضد ویروس به زبان های انگلیسی، آلمانی، اسپانیایی، ایتالیایی، پرتقالی، چکسلواکی و لهستانی قابل دسترس می باشد. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:



شرکت سازنده	ESET SOFTWARE
آدرس شرکت	Coronado, USA
آدرس وب سایت	www.nod32.com
آیا امکان تست رایگان وجود دارد؟	بله، ۳۰ روز رایگان
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	خیر
بلوکه کنندهٔ اسپم ها	خیر
بلوکه کنندهٔ تبلیغات	خیر

برنامهٔ ضد ویروس *Norton*

یکی از با سابقه ترین برنامه های ضد ویروس، برنامهٔ ضد ویروس Norton محصول شرکت Symantec می باشد. این شرکت را می توان یکی از اولین **شرکت های تولید کنندهٔ برنامه های ضد ویروس** برای کامپیوترهای خانگی دانست. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:

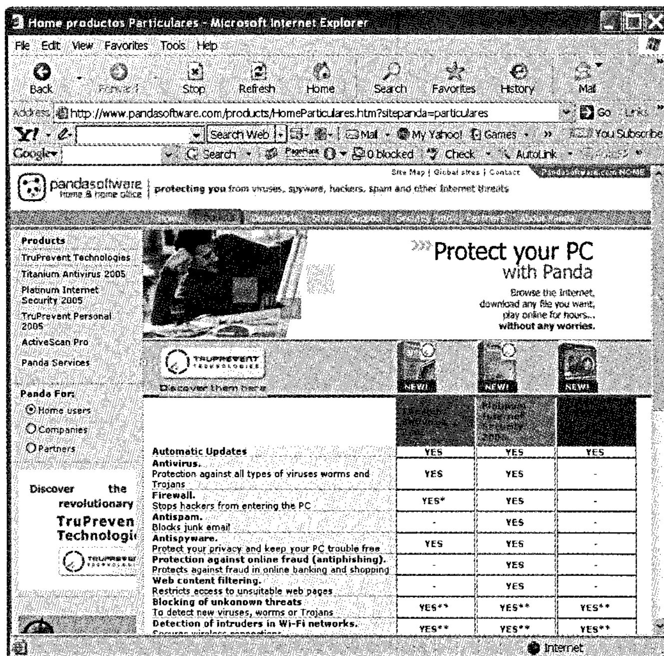


شرکت سازنده	SYMANTEC
آدرس شرکت	Cupertion, CA, USA
آدرس وب سایت	www.symantec.com
آیا امکان تست رایگان وجود دارد؟	بلـه، ۹۰ روز از طریـق وب سـایت www.symantec.com/downloads
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله، از طریق مراجعه به وب سایت www.symantec.com/securitychek
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندهٔ اسپم ها	بله
بلوکه کنندهٔ تبلیغات	بله

برنامهٔ ضد ویروس *Panda*

یکی از جالب ترین برنامه های ضد ویروس، پاندا محصول شرکت Panda Software مـی باشـد. ایـن شرکت با **تولید اشکال مختلفی از ضد ویروس** پاندا امکانـات متنـوعی را در اختیـار کـاربران قـرار می‌دهد.

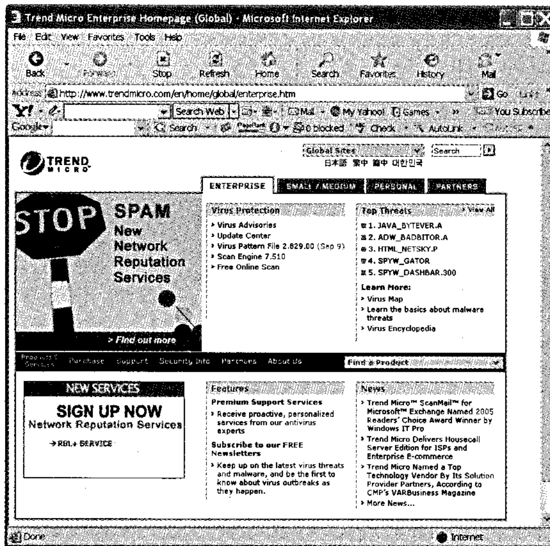




شرکت سازنده	PANDA SOFTWARE
آدرس شرکت	Bilbao, Spain
آدرس وب سایت	www.pandasoftware.com
آیا امکان تست رایگان وجود دارد؟	بلــه، ۹۰ روز از طریــق وب ســایت www.pandasoftware.com/microsoft/english
آیا امکان خرید **Online** وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت **Online** برای کاربران وجود دارد؟	بله، از طریق مراجعه به وب سایت www.pandasoftware.com/activescan
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندهٔ اسپم ها	بله
بلوکه کنندهٔ تبلیغات	خیر

برنامهٔ ضد ویروس *PC-Cillin*

یکی از برنامه های مفید که دارای قابلیت های متعددی جهت **کشف** و **حذف** ویروس ها می باشد برنامهٔ PC-Cillin می باشد. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:



شرکت سازنده	TEND MICRO INC
آدرس شرکت	Tokyo, Japan
آدرس وب سایت	www.trendmicro.com
آیا امکان تست رایگان وجود دارد؟	بله، ۳۰ روز
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله، از طریق مراجعه به وب سایت housecall.trendmicro.com
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	
فایروال	بله
بلوکه کنندهٔ اسپم ها	بله
بلوکه کنندهٔ تبلیغات	بله

برنامهٔ ضد ویروس ایمن

یکی از با سابقه ترین برنامه های ضد ویروس در ایران، ضد ویروس ایمن می باشد. شرکت مهران رایانه با ارائهٔ این ضد ویروس و تولید آن در اشکال مختلف تحت Dos، تحت شبکه و تحت ویندوز گامی نو در جهت مقابله با ویروس های کامپیوتری در ایران برداشته است. از ویژگی های دیگر این ضد ویروس، می توان به قابلیت دو زبانه بودن فارسی/انگلیسی آن اشاره کرد. جدول ویژگی های این برنامهٔ ضد ویروس به شرح زیر است:



شرکت سازنده	شرکت مهندسی مهران رایانه
آدرس شرکت	ایران-تهران-خیابان جمهوری
آدرس وب سایت	www.ImenAntiVirus.com
آیا امکان تست رایگان وجود دارد؟	بله
آیا امکان خرید Online وجود دارد؟	بله
آیا امکان دانلود اطلاعات یا برنامه از طریق وب سایت وجود دارد؟	بله
آیا امکان اسکن به صورت Online برای کاربران وجود دارد؟	بله
بسته نرم افزاری این برنامه شامل چه چیزهایی است؟	

فایروال	بله
بلوکه کنندهٔ اسپم ها	بله
بلوکه کنندهٔ تبلیغات	بله

بیشتر بدانیم: ویروس خودکشی بن لادن

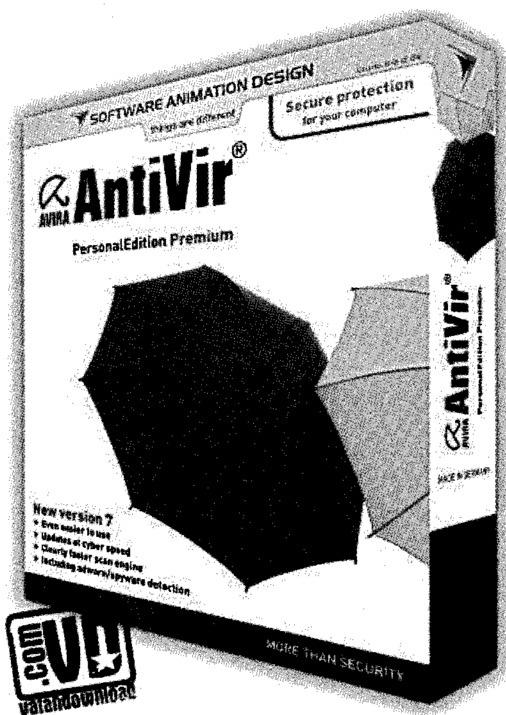
یکی از ویروس های مخربی که در سال های اخیر شاهد آن بودیم ویروسی به نام خودکشی بن لادن بود. این ویروس در غالب یک **E-mail** که ادعا می کرد حاوی تصاویری از خودکشی بن لادن است در تمام دنیا انتشار یافت. عنوان جالب این پیغام باعث آلودگی کامپیوترهای زیادی شد. نوآوری جالب در این ویروس استفاده از علایق روز مردم دنیا به عنوان پیغام خود می باشد.

برنامهٔ ضد ویروس *Avira*

یکی از ضدویرس‌های بسیار کارآمد که توانسته است جایگاه ویژه‌ای را در بین کاربران کامپیوتر برای خود تست و پا کند برنامهٔ ضدویروس Avira است. این ضدویروس یک ابزار کارآمد برای محافظت در مقابل ویروس‌ها، بدافزارها و ... است. طبق آمارهای سایت AV-computeratives این ضدویروس با قدرت تشخیص ۹۹/۶٪ به عنوان بهترین ضدویروس سال ۲۰۰۸ معرفی شده است. این ضدویروس نسبت به ضدویروس‌های Nod32 و Kaspersky از سطح امنیتی بالاتری برخوردار است.

این ضدویروس بر اساس آزمایش‌های انجام شده دارای بالاترین رتبه در اسکن کردن و پیش‌گیری از آلوده شدن است.





شرکت سازنده	AVIRA
آدرس وب سایت	www.free.av.com
آیا امکان تست رایگان وجود دارد؟	بله، تا زمانیکه می‌خواهید آنرا Update کنید.
عملکرد	قتل عام تمامی ویروس‌ها
مزایا	شناسایی اکثر ویروس‌ها-سادگی برنامه- سرعت بالا- حجم کم و کند نکردن سرعت ویندوز
معایب	امکان بازسازی فایل‌های آلوده تنها در نسخهٔ پولی آن وجود دارد و همچنین در نسخهٔ رایگان قابلیت بررسی POP3 و Antispy ware وجود ندارد.
آیا امکان به‌روزسازی وجود دارد؟	بله
اندازهٔ آنتی‌ویروس	حدود ۲۴ مگابایت

خلاصهٔ این فصل

این فصل، پنجره ای تازه از مهترین برنامه های ضد ویروس دنیای کامپیوتر را در پیش روی ما گشود. ویژگی های ذکر شده در این فصل می تواند در انتخاب و مقایسهٔ قابلیت های مختلف برنامه های ضد ویروس توسط کاربران تأثیر فراوانی داشته باشد. حالا با توجه به نیازهای خود قادرید به راحتی برنامهٔ ضد ویروس را برای خود تهیه کرده و آن را بر روی کامپیوتر خود نصب کنید.

☺ همراه: مقصود از قابلیت های شناخت ویروس های محلی، شناخت ویروس هایی است که در داخل کشور ایران تولید و ارائه می گردد. متأسفانه این ویروس ها به وسیلهٔ اکثر برنامه های ضد ویروس شناخته می شود ولی به دلیل عدم شناسایی دقیق این ویروس ها، اکثر برنامه های ضد ویروس قابلیت از بین بردن آنها را دارا نمی باشند.

«سخنان درگوشی»

آیا ویروس‌ها می‌توانند صدمات فیزیکی به قطعات سخت‌افزاری وارد کنند؟!

در این مورد ویروسی به نام CIH وجود داشت که Firmware و یا BIOS کامپیوتر را آلوده می‌کرد، اما به سخت‌افزار سیستم آسیبی وارد نمی‌کرد. شایعات در مورد ویروس‌هایی که کامپیوتر را دیوانه می‌کنند و موجب انفجار آن می‌شوند، زیاده‌گویی و تا حدودی هم خنده‌دار است. اگر احیاناً کامپیوتر شما به خاطر یکی از این ویروس‌ها از کار بیفتد، نهایتاً مجبور هستید آن را پیش یک متخصص ببرید تا بایوس سیستم شما را جایگزین کند، اما این مشکل اصلاً منجر به این نمی‌شود که سیستم‌تان به خاطر آن ویروس به قتل برسد.

فصل ۹

داستان‌هایی در مورد ویروس‌ها

ویروس های کامپیوتری برنامه هایی هستند که به روش ها و سبک های مختلفی کامپیوترها را مورد حمله قرار می دهند. در این فصل ما قصد نداریم داستان سرایی کرده و درمورد خطرات ورود ویروس ها به کامپیوترتان صحبت کنیم چون مطمئن هستیم شما داستان شنگول و منگول را خوانده‌اید و با تجاربی که تا اینجای کتاب بدست آورده اید با این خطرات و روش های مقابله با آنها آشنا شده اید.

ما در این قسمت از کتاب قصد داریم مجموعه سئوالاتی را که ممکن است در ذهن شما پیش آمده باشد را مرور کرده و به همراه هم جوابی مناسب برای این سئوالات پیدا کنیم. این سئوالات شاید همان پرسش هایی باشد که در ذهن شما پیش آمده است.

داستان اول

در یکی از جراید آمده است که هر ویروس شناخته شده کامپیوتری دارای شناسه و اصطلاحاً امضایی(Signature) می باشد. لطفاً در مورد این شناسه کمی توضیح دهید.

ویروس باشی: ویروس شناخته شده اصطلاحاً به ویروسی اطلاق می شود که به وسیلهٔ شرکت‌های تولید کنندهٔ ضد ویروس شناسایی شده باشد. اکثر این ویروس ها یا خود دارای اسمی هستند و یا بر اساس شکل و ظاهر حمله، اسم گذاری می شوند. هر ویروس کامپیوتری دارای **مجموعه بایت های شناخته شده ای** می باشد که با شناسایی آنها توسط برنامه های ضد ویروس کمک شایانی می کند و به آنها امضا یا مشخصهٔ ویروس می گویند.



داستان دوم

صداهای عجیب و غریبی از بلند گوی کامپیوترم بلند می شود به طوریکه من گاهی تصور می کنم که کامپیوترم جن زده شده است. به نظر شما به وسیلهٔ برنامه های ضد ویروس می توان کامپیوترم را نجات داد؟

ویروس باشی: لازم نیست دچار ترس و وحشت شوید به احتمال زیاد کامپیوتر شما ویروسی شده است. برای این منظور شما می توانید از یک برنامهٔ ضد ویروس معتبر استفاده کنید. ویروس ها نشانه های عجیب و غریب دیگری مثل ایجاد اختلال در کار چاپگر یا جلوگیری از دسترسی به یکی از درایوها را نیز دارند.



داستان سوم

کامپیوتر من بسیار خوب کار می کرد ولی امروز به یکباره قفل کرد و دیگر هیچ کاری با آن نتوانستم انجام دهم. به نظر شما آیا کامپیوتر من ویروسی است؟

ویروس باشی: از کار افتادن کامپیوترها و متعاقباً قفل کردن توسط ویروس های کامپیوتری، یک فرایند سلسله وار است که بر اساس یک پروسهٔ زمانی حادث می شود. بله کامپیوتر می تواند بر اساس عملیات تخریبی یک ضد ویروس از کار بیافتد ولی نه همیشه. برای یک ویروس بهتر آن است که یک کامپیوتر فعالیت کند تا از کار بیافتد.

داستان چهارم

چرا بعضی از گونه های یک ویروس را هیچ ضد ویروسی حتی ضد ویروس‌های محلی نمی‌تواند پاکسازی کند و حتی برنامه های ضد ویروس در حین پاکسازی قفل می کنند؟

ویروس باشی: این مسئله می تواند ناشی از آلوده سازی ناقص فایل مورد نظر توسط یک ویروس و یا عملکرد چندین ویروس باشد. در نتیجه اطلاعات اولیهٔ فایل از بین رفته و غیر قابل بازگشت می‌باشد. بنابراین با نهایت تأسف باید عرض کنم تنها راه باقی مانده حذف فایل مربوطه می باشد.

داستان پنجم

چرا بعد از کشتن ویروس One Helf ، بعضی از دایرکتوری ها خالی می شوند و یا فایل هایی با نام های نامفهوم و با ظرفیت های باور نکردنی به وجود می آیند؟

ویروس باشی: زیرا این ویروس علاوه بر آلوده کردن فایل ها، اطلاعات هارد دیسک را نیز کد می‌کند. بنابراین اگر صرفاً فایل های آلوده به این ویروس پاکسازی شده و اطلاعات کد شده بازیابی نگردند، کاربر با دایرکتوری ها و فایل های با مشخصات فوق مواجه می گردد.



داستان ششم

گاهی اوقات برنامه های ضد ویروسی مثل ایمن پیغام می دهند که ویروس پیدا شده در حافظهٔ غیر فعال می باشد. آیا در این حالت خطری متوجه سیستم می باشد؟

ویروس باشی: این پیغام وقتی نمایش داده می شود که واقعاً ویروسی در حافظه بوده باشد و ضد ویروس پس از پیدا کردن آن ویروس فوق را در حافظه غیر فعال کرده باشد. در این حالت لازم نیست نگران باشید هیچ گونه خطری متوجه سیستم شما نمی باشد. در این مواقع بهتر است سیستم کاملاً بررسی شود تا چنانچه فایل آلوده ای وجود داشته باشد پاکسازی گردد.

داستان هفتم

چگونه می توان یک فلاپی دیسک را ویروس زدایی کرد؟

ویروس باشی: برای پاک سازی ویروس های موجود بر روی فلاپی دیسک کافی است پس از اجرای برنامهٔ ضد ویروس (مثلاً ایمن) و نمایان شدن صفحهٔ اصلی آن به صورت کامل، دیسکت ضد

ویروس را از درون درایو خارج کرده و فلاپی مورد نظر را در درون درایو قرار دهید. سپس با انتخاب فلاپی درایو از طریق گزینهٔ انتخاب درایو نسبت به پاک سازی فلاپی اقدام کنید.

خلاصهٔ این فصل

در این فصل ما داستان های زیادی را در مورد ویروس ها شنیدیم (از جن زده شدن کامپیوتر شما تا قفل کردن آن). راستی کدامیک از این سئوالات در ذهن شما پیش آمده بود؟ در هر حال امیدواریم جواب های مناسبی را برای سئوالات خود پیدا کرده باشید.

«سخنان درگوشی»

پرسه در دالان سیاه اینترنت

دست کم نیمی از جرائم و تبهکاری های اینترنتی به صورت سازمان یافته انجام می شوند. تولید ویروس ها و کدهای مخرب، انتشار ابزار هک و نرم افزارهای نفوذ، تکثیر و ارسال هرزنامه ها و هر نوع خرابکاری دیگری که فکرش را بکنید. اما در این بین، کسب درآمدهای نامشروع، سرقت و نقل و انتقال غیرقانونی پول در اینترنت، جرائمی هستند که تقریباً به طور کامل به گروه های سازمان یافته و مافیایی وابسته اند. این گروه های تبهکاری بازار خرید و فروش اطلاعات ارزشمند کاربران و یا شریان نقل و انتقال پول های غیر قانونی در اینترنت را کنترل می کنند. شبکه هایی اغلب وسیع از تولید کنندگان و فروشندگان ابزارهای خرابکاری در اینترنت و دلالان اطلاعات رایانه ای که در صدها مرکز تولید و مجموعه فروشگاهی آنلاین به انتشار بی وقفه نرم افزارهای مخرب و ابزار هک می پردازند. این یک تجارت حرفه ای و صنعت سودآور است که هر روز کاربران بیشتری را جذب خود می کند. البته اغلب این اعضاء جدید الورود را جوانان و نوجوانان غیر حرفه ای تشکیل می دهند که در ابتدا به انجام فعالیت های مخرب به صورت تفریحی علاقه دارند. اما رفته رفته و پس از مدت کوتاهی به یک مجرم اینترنتی با تجربه و حرفه ای تبدیل می شوند. برای اینکه با وضعیت جرائم سازمان یافته در اینترنت بیشتر آشنا شویم. نگاهی می اندازیم به جدیدترین گزارش شرکت امنیتی Panda Security که در خصوص شبکه های بزرگ تبهکاری اینترنتی منتشر شده است.بازار سیاه جرائم اینترنتی ، که به صورت سنتی بر خرید و فروش اطلاعات مسروقه، مانند اطلاعات بانکی و داده های محرمانه شخصی و سازمانی متمرکز بوده، اکنون به مراکز بزرگ تولید نرم افزارهای مخرب، مراکز بحث و بررسی روش های تخریب و حتی اتاق های فکر برای تغییر استراتژی های ضد امنیتی تبدیل شده است. البته حاصل دسترنج این همه فعالیت، صدها مجموعه فروشگاهی آنلاین برای عرضه انواع اطلاعات محرمانه و ابزار نفوذ و نیز راهکارهای شناسایی ضعف های امنیتی در تجهیزات رایانه ای بوده است که همگی در نیمه تاریک اینترنت متولد شده اند.

با ورود به این مجموعه های فروشگاهی شما به انبوهی از اطلاعات سرقت شده دسترسی خواهید داشت که تا قبل از کشف فعالیت های خرابکارانه شما توسط نهادها یا شرکت های امنیتی به شما کمک می کنند تا

درآمدهای کلان، البته از راهی غیر قانونی، کسب کنید. برای مثال با پرداخت تنها ۲ دلار، به اطلاعات محرمانه یک کارت اعتباری مانند نام کاربری و رمز عبور دسترسی خواهید داشت. البته برای اطلاع از جزییات بیشتر این حساب مانند موجودی، صورت وضعیت و یا اصولاً جاری بودن و اعتبار خود حساب، نیاز به پرداخت پول بیشتری خواهید داشت: به طور متوسط ۸۰ دلار برای حساب های کوچکتر و کم اهمیت تر و تا ۷۰۰ دلار برای حساب هایی که دست کم ۸۲۰۰۰ دلار موجودی دارند. در این بین ممکن است شما پیشنهادهای عجیب دیگری هم دریافت کنید. تعجب نکنید چون ، دستگاه های ATM مجازی برای برداشت پول از کارت های اعتباری سرقت شده (۳۵۰۰ دلار)، ابزار بازتولید کارت های اعتباری برای تایید اعتبار اطلاعات کاربری (۲۰۰ تا ۱۰۰۰ دلار) و از آن عجیب تر خدمات پولشویی اینترنتی (مانند حواله های بانکی و یا چک های نقدی با کسر ۱۰ تا ۴۰ درصد از اصل پول سرقت شده و مورد انتقال) نیز در میان اقلام قابل عرضه قرار دارند ! به خاطر داشته باشید که هر لحظه امکان از دست رفتن دسترسی به این حساب ها و ابزار وجود دارد، که مهمترین دلیل آن کشف فعالیت مجرمانه شما توسط نهادها یا شرکت های امنیت اینترنت است. در کنار این خرده فروشی ها (!)، معمولاً معامله های بزرگی نیز جریان دارند که شامل خرید و فروش نقشه ها و پروژه های کلان تخریبی در اینترنت هستند. این پروژه های عملیاتی، معمولاً امن تر هستند و به سرقت های وسیع تر و بازده مالی بالاتر منجر می شوند. اگر شما خود یک تبهکار با تجربه و حرفه ای باشید می توانید به صورت توافقی مبلغ این پروژه ها را بپردازید و کار را شروع کنید. تولید فروشگاه های اینترنتی تقلبی و اجرای کلاهبرداری‌های آنلاین، تولید و انتشارضد ویروس های جعلی، انتشار وسیع لینک های آلوده برای فعالسازی ابزار نفوذ و ... می توانند تنها بخشی از این پروژه های تخریبی آماده باشند. جالب این که شما می توانید با پرداخت مبالغ بیشتر وب سایت های جعلی ، صفحات مخرب و لینک های آلوده خود را از طریق تکنیک‌های پیشرفته در میان نتایج اول و صفحات نخست موتورهای جستجو قرار دهید ! در بازارهای سیاه جرائم سایبر، شما می توانید حتی یک شبکه Botnet را نیز خریداری یا اجاره کنید. این شبکه ها معمولاً مجموعه ای وسیع از رایانه‌های آلوده و تحت فرمان هستند که برای ارسال هرزنامه های تبلیغاتی یا نامه های آلوده به ابزار نفوذ در مقیاس‌های وسیع بکار می‌روند. نگران نباشید! برای ناشناس ماندن شما نیز همیشه راهی وجود دارد. پیشنهاد این تبهکاران، اجاره یک سرور SMTP و یا یک خط VPN با پرداخت حداکثر ۲۰ دلار برای سه ماه است تا شما از شناسایی، پی گیری و تعقیب قانونی معاف بمانید. اما شاید جالب ترین نکته در این بازار مکاره، رقابت شدید میان تولیدکنندگان و ارائه دهندگان ابزار تخریبی باشد. درست مانند هر نوع تجارت دیگر اینجا حق همیشه با مشتری ست (!) و نیازهای اوست که راهبرد بازار را تعیین می کند. بنابراین قیمت پروژه های تخریب، ابزار هک و نفوذ و سایر راهکارهای مخرب در سطح رقابتی و در پایین ترین حد ممکن نگاه داشته می شود، حق استفاده از نسخه‌های آزمایشی محصولات برای مشتری محفوظ است و در برخی موارد، برگشت پول در صورت عدم رضایت از کیفیت عملکرد نیز ضمانت می شود! به نظر می رسد که کسب و کار زیرزمینی و غیرقانونی در نیمه تاریک اینترنت از رونق مناسبی برخوردار است ، البته تا آن هنگام که کاربران رایانه و اینترنت، از آگاهی امنیتی کافی و امنیت آگاهانه لازم برخوردار نباشند. بنابراین برای این که همواره در نیمه پاک و روشن اینترنت باقی بمانیم، اجباراً باید فکری به حال امنیت رایانه های خود بکنیم. راه های نفوذ را ببندیم. از پیشرفته‌ترین فن آوری حفاظتی استفاده کنیم. بد نیست کمی هم بدبین یا حساس باشیم زیرا ممکن است بدون هیچ نشانه و علامتی، رایانه‌های ما همین حالا تحت فرمان یک تبهکار اینترنتی با تجربه باشد و ما ناخواسته به تکثیر آلودگی در اینترنت بپردازیم.

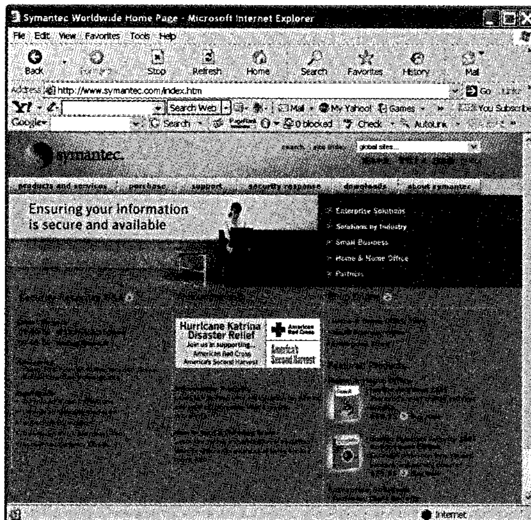
فصل ۱۰

معرفی برنامهٔ ضدویروس Norton

یکی از با سابقه ترین برنامه های ضد ویروس برنامهٔ Norton محصول شرکت Symantec می باشد.
این برنامهٔ ضد ویروس با قابلیت های فراوانی که به کاربران هدیه می کند جایگاه ویژه ای در بین علاقه مندان برنامه های ضد ویروس دارد.

از ویژگی های منحصر به فرد این برنامهٔ ضد ویروس می توان به قابلیت ویروس یابی اتوماتیک، دارا بودن فایروال، بلوکه کنندهٔ اسپم ها و بلوکه کنندهٔ تبلیغات، اشاره کرد.

خوشبختانه شما به سادگی می توانید نسخهٔ اصلی این برنامهٔ ضد ویروس را از نمایندگی آن در کشورمان تهیه کنید.



☺ بیشتر بدانیم: سیستم مورد نیاز برای نصب و استفادهٔ صحیح از برنامهٔ ضد ویروس **Norton** چه سیستمی است؟

شما برای نصب و استفاده از حداکثر قابلیت های برنامهٔ ضد ویروس **Norton** به امکانات زیر نیاز دارید:

- دارا بودن ریزپردازنده ای با سرعت ۱۳۳ مگاهرتز یا بالاتر
- دارا بودن ۶۴ مگابایت **RAM** یا بیشتر
- دارا بودن ۸۵ مگابایت حافظه از هارد دیسک

گام اول: فعال کردن پنجرهٔ اصلی ضدویروس Norton

در اولین ایستگاه آشنایی با برنامهٔ ضد ویروس Norton نگاهی گذرا به پنجرهٔ اصلی این برنامه خواهیم داشت. یکی از ویژگی های جذاب این برنامه سادگی و زیبایی پنجرهٔ اصلی برنامه می باشد.

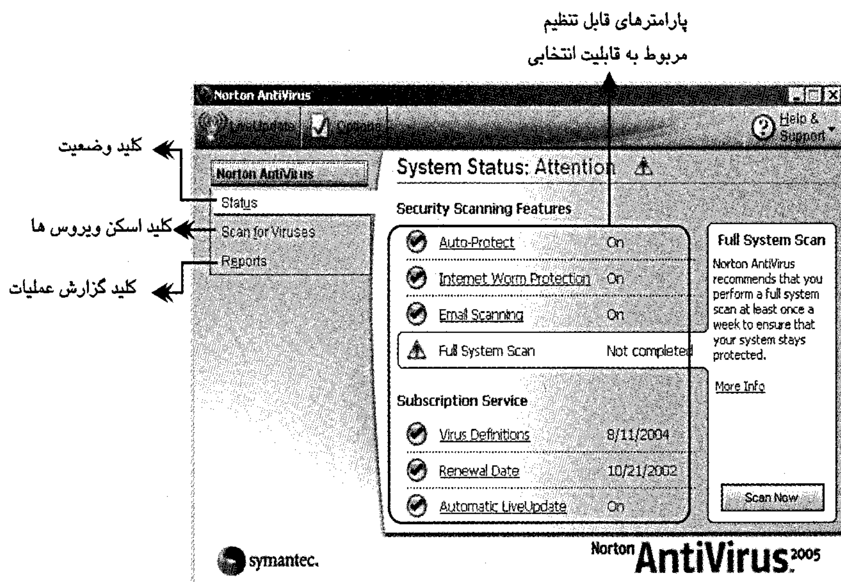
☺ همراه: ما در این کتاب به بررسی آخرین نسخهٔ برنامهٔ ضد ویروس **Norton** یعنی نسخهٔ **Norton 2005** پرداخته ایم. ممکن است هنگامی که شما این کتاب را مطالعه می کنید این نسخهٔ ضد ویروس بروز شده باشد. لازم نیست شما نگران این مسئله باشید اصول کلی برنامهٔ ضد ویروس در نسخهٔ جدید برنامه نیز قابل استفاده است.

باز کردن پنجرهٔ برنامه

برای باز کردن پنجرهٔ اصلی برنامهٔ ضد ویروس شما می توانید از سه روش زیر بهره ببرید:

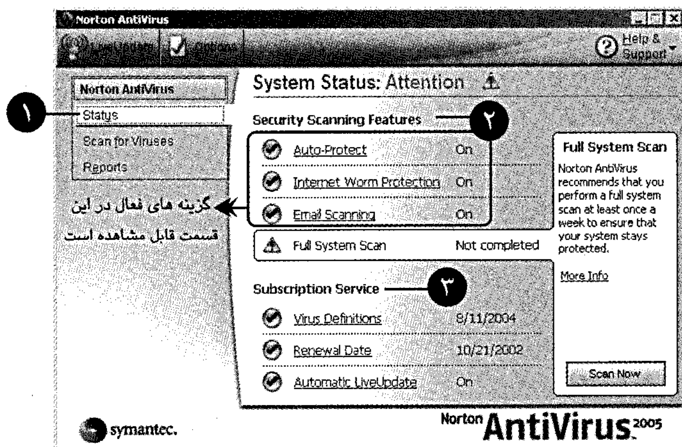
- بر روی آیکون میانبر برنامه (■) در صفحهٔ رومیزی دوبار کلیک کنید.
- بر روی آیکون برنامه (■) در کنار ساعت کامپیوتر کلیک کنید.
- دستورات Start→All Programs→Norton Anti Virus 2005 را انتخاب کنید.

در این حالت پنجره ای به اسم Norton Anti Virus در روی صفحهٔ نمایش ظاهر می شود.



گام دوم: بررسی وضعیت فعلی ضدویروس

یکی از اولین کارهایی که شما هنگام باز کردن پنجرهٔ اصلی برنامه باید بـه آن توجـه کنیـد وضـعیت جاری برنامهٔ ضد ویروس می باشد. بـرای دسـتیابی بـه وضـعیت موجـود بـر روی کلیـد وضـعیت (Status) در پنجرهٔ اصلی برنامه کلیک کنید. با کلیک کردن بر روی این کلید، لیست وضعیت برنامه در سمت راست پنجره نمایان می گردد.



۱- بر روی کلید وضعیت کلیک کنید. ۲- جزئیات امنیتی ضد ویروس ۳- سرویس های زیر مجموعه

جزئیات امنیتی ضد ویروس شامل گزینه هایی به شرح زیر می باشد:

☑ **گزینهٔ Auto Protect**: فعال بودن این گزینه امکان مقابلهٔ اتوماتیک برنامهٔ ضد ویروس با ویروس های ورودی به کامپیوتر را فراهم می کند. ویروس ها از روش ها و امکانات مختلفی جهت ورود به سیستم بهره می گیرند رایج ترین این روش ها از طریق شبکهٔ اینترنت، به وسیلهٔ رسانه های انتقال اطلاعات مثل CD و فلاپی دیسک می باشد.

☑ **گزینهٔ Internet Worm Protection**: فعال بودن این گزینه، امکان مقابله با نفوذ کرم های اینترنتی به کامپیوتر شما را برای برنامهٔ ضد ویروس فراهم می کند.

☑ **گزینهٔ Email Scanning**: فعال بودن این گزینه، امکان مقابله با ویروس های پیوستی به E-mail ها را برای ضد ویروس میسر می سازد.

☑ **گزینهٔ Full System Scan**: این گزینه نمایش دهندهٔ وضعیت اسکن کامپیوتر شما توسط برنامهٔ ضد ویروس می باشد.

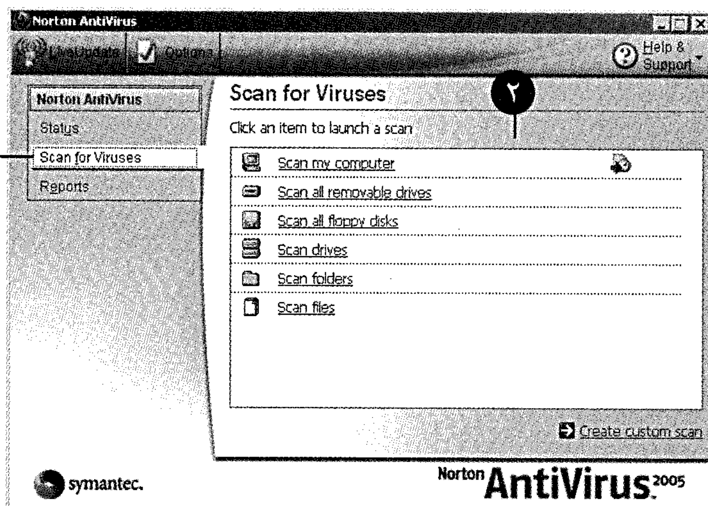
> ☺ **همراه: فعال بودن هر گزینه با On و غیر فعال بودن هر گزینه با Off نشان داده می شود.**

سرویس های زیر مجموعه، شامل سه گزینه به شرح زیر می باشند:

- **گزینهٔ Virus Definition**: این گزینه آخرین وضعیت بروز سازی اطلاعات ضد ویروس جهت مقابله با ویروس را نمایش می دهد.
- **گزینهٔ Renewal Date**: این گزینه آخرین تاریخ به روز سازی ضد ویروس را نمایش می دهد.
- **گزینهٔ Automatic Live Update**: فعال بودن این گزینه نشان دهندهٔ قابلیت به روزسازی اتوماتیک برنامهٔ ضد ویروس می باشد.

گام سوم: ویروس‌یابی به وسیلهٔ Norton

در این ایستگاه ما قصد داریم روش ویروس زدایی به وسیلهٔ برنامهٔ ضد ویروس Norton را بررسی کنیم. برای استفاده از این قابلیت برنامهٔ ضد ویروس، گزینهٔ Scan for Viruses را کلیک کنید تا پارامترهای قابل انتخاب آن در سمت راست پنجرهٔ برنامه فعال گردد:

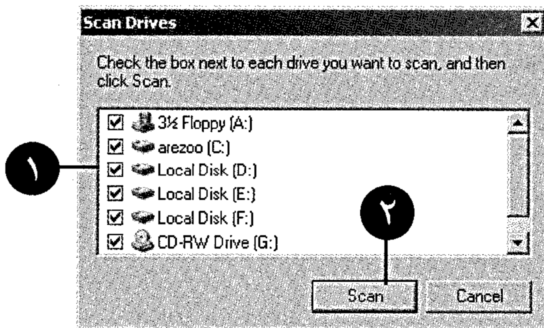


۱- پارامترهای قابل انتخاب

۲- جهت ویروس یابی این گزینه را کلیک کنید.

لیست پارامترهای قابل انتخاب در پنجرهٔ فوق امکان تنظیم دقیق موضوعات مورد نظرتان جهت اسکن را برای شما فراهم می کند. پارامترهای موجود در این لیست شامل موارد زیر می باشد:

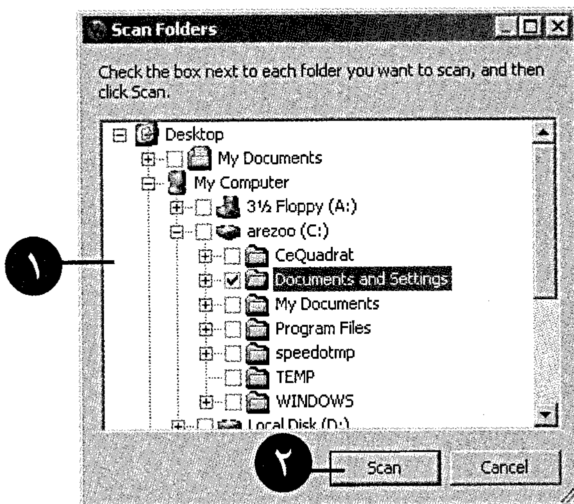
- **Scan my computer**: با انتخاب این پارامتر کل محتویات کامپیوتر شما جهت ویروس یابی اسکن می شود.
- **Scan all removable drives**: با انتخاب این پارامتر کلیهٔ درایوهای قابل جابجایی اسکن می شود.
- **Scan all floppy disks**: با انتخاب این پارامتر کلیهٔ فلاپی دیسک های کامپیوتر اسکن می شود.
- **Scan drives**: با انتخاب این پارامترها پنجره ای در روی صفحهٔ نمایش ظاهر می شود که امکان انتخاب درایو مورد نظرتان را جهت اسکن به شما می دهد.



۱- درایو مورد نظرتان را از این لیست انتخاب کنید.

۲- کلید Scan را کلیک کنید.

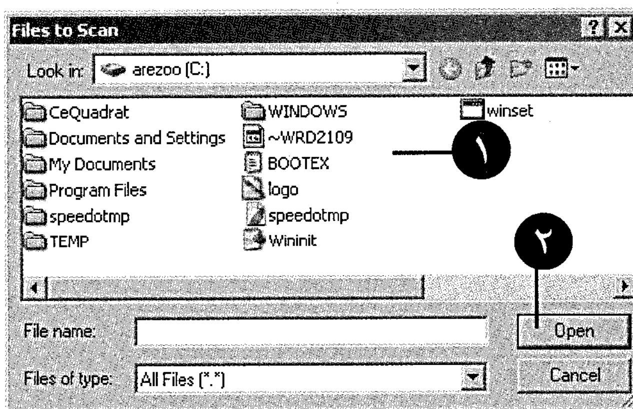
• **Scan folders**: با انتخاب این پارامتر پنجره ای در روی صفحهٔ نمایش ظاهر می شود که به شما امکان انتخاب پوشهٔ مورد نظرتان جهت اسکن را می دهد.



۱- از این لیست پوشهٔ مورد نظرتان را انتخاب کنید.

۲- کلید **Scan** را انتخاب کنید.

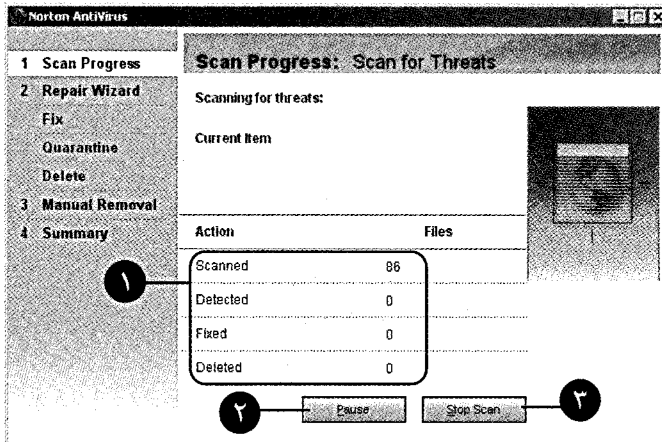
• **Scan Files**: با انتخاب این پارامتر پنجره ای در روی صفحهٔ نمایش ظاهر می شود که به شما امکان انتخاب فایل های مورد نظرتان را جهت اسکن می دهد.



۱- فایل های مورد نظرتان را از این قسمت انتخاب کنید.

۲- کلید **Open** را انتخاب کنید.

برای انتخاب هر یک از این گزینه ها کافی است بر روی آن کلیک کنید. در این حالت پنجره ای در روی صفحهٔ نمایش ظاهر می شود که فرایند اسکن را نمایش می دهد.

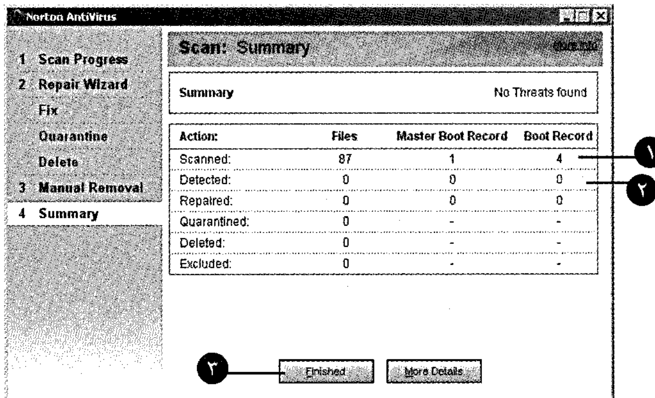


۱- وضعیت اسکن در این لیست قابل مشاهده است.

۲- جهت توقف موقت ویروس یابی کلید Pause را کلیک کنید.

۳- برای توقف کامل اسکن، کلید Stop Scan را انتخاب کنید.

پس از چند لحظه (بسته به حجم و اندازهٔ فایل، درایو و یا پوشهٔ انتخابی) پنجره ای نتیجهٔ ویروس یابی را به شما گزارش می دهد.



۱- تعداد فایل های اسکن شده در این قسمت قابل مشاهده است.

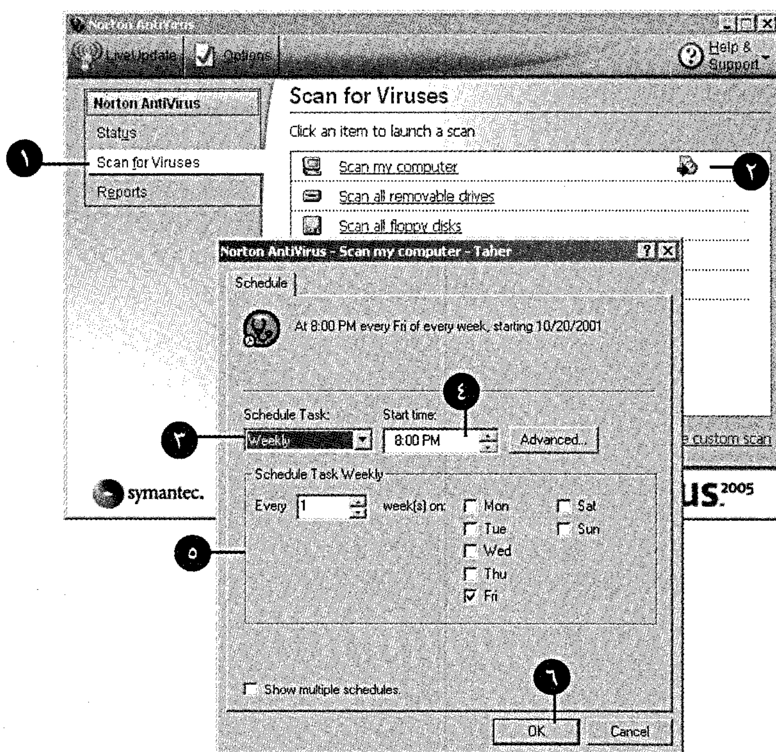
۲- تعداد ویروس های یافته شده در این قسمت نمایش داده می شود.

۳- برای اتمام فرایند، کلید Finished را انتخاب کنید.

گام چهارم: تنظیم یک زمان‌بندی اتوماتیک جهت اسکن

یکی از قابلیت های جذاب این ضد ویروس، قابلیت تنظیم یک برنامهٔ زمان بندی جهت اسکن محتویات کامپیوتر می باشد. استفاده از قابلیت زمان بندی اتوماتیک برنامهٔ ضد ویروس جهت اسکن، کارآیی و امنیت سیستم را تا حد زیادی بالا می برد. در این گام ما قصد داریم با تأملی چند نگاهی کنجکاوانه به این قابلیت برنامه در تنظیم زمان بندی اتوماتیک داشته باشیم.

برای این منظور پنجرهٔ اصلی برنامهٔ ضد ویروس را باز کرده و گزینهٔ Scan for Viruses را انتخاب کنید.



۱- گزینهٔ Scan for Viruses را انتخاب کنید.

۲- روی آیکون ساعت در این قسمت کلیک کنید.

۳- دورهٔ زمانی مورد نظرتان جهت اسکن اتوماتیک را از این منوی کشویی انتخاب کنید.

۴- ساعت اسکن را در این قسمت وارد کنید.

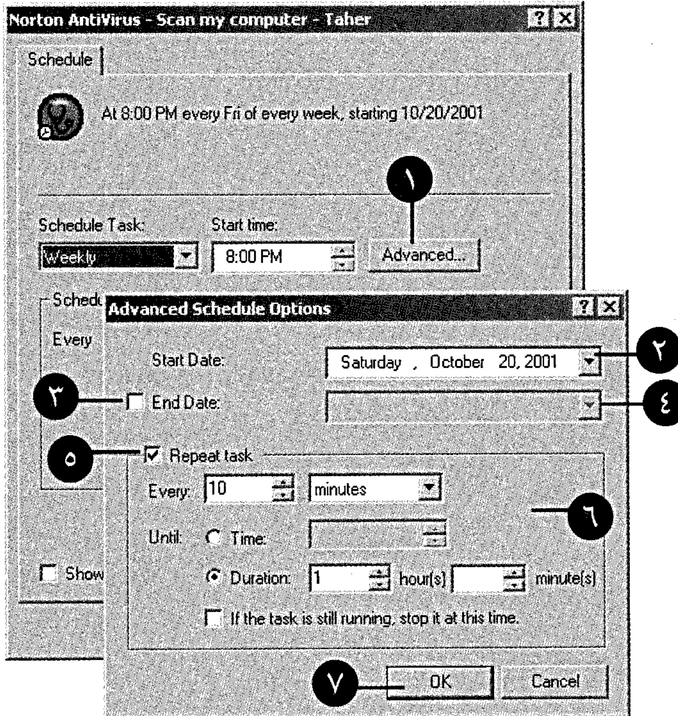
۵- این پارامترها با توجه به نوع دورهٔ زمانی تغییر می کند.

۶- برای اتمام فرایند زمان بندی کلید OK را کلیک کنید.

☺ همراه: با توجه به دورهٔ زمان بندی انتخابی (مثل روزانه، هفتگی، ماهانه و ...) پارامترهای ظاهر شده در قسمت Schedule Task Weekly تغییر می کند.

تنظیمات پیشرفتهٔ زمان بندی

برای اعمال تنظیمات پیشرفتهٔ زمان بندی بر روی کلید Advanced در پنجرهٔ زمان بندی کلیک کنید.



۱- کلید **Advanced** را کلیک کنید.

۲- تاریخ شروع اسکن را به صورت دقیق از این منوی کشویی انتخاب کنید.

۳- این گزینه را فعال کنید.

۴- تاریخ اتمام دورهٔ اسکن را از این منوی کشویی انتخاب کنید.

۵- برای تکرار فرایند زمان بندی این گزینه را فعال کرده و ...

۶- تنظیمات مربوطه را از این منوی کشویی انتخاب کنید.

۷- کلید **OK** را انتخاب کنید.

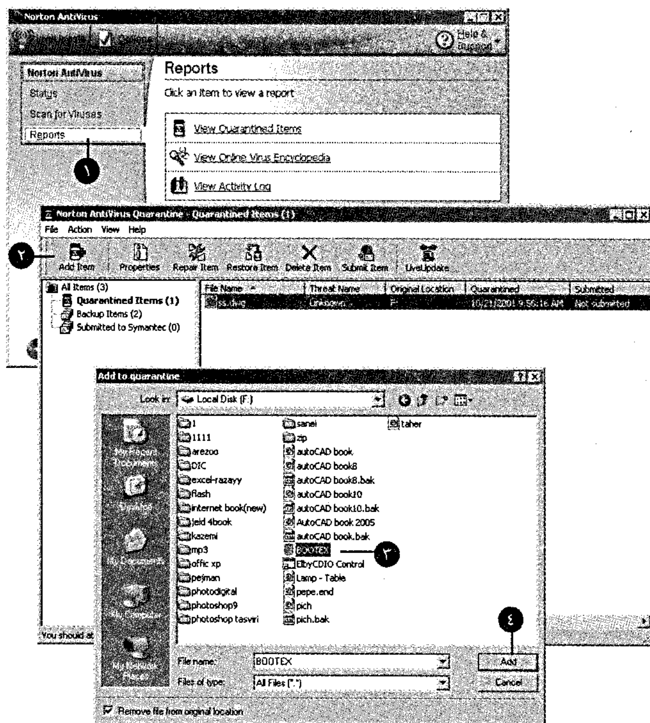
☺ همراه: همان طور که قبلاً نیز به صورت مکرر به آن اشاره شد استفاده از زمان بندی اتوماتیک، ضریب امنیتی اطلاعات کامپیوتر را تا حد زیادی بالا می برد بنابراین، این قابلیت را سر لوحهٔ کار خود قرار دهید.

گام پنجم: قرنطینه کردن فایل‌های آلوده

با استفاده از قابلیت قرنطینه سازی فایل های آلوده در برنامهٔ ضد ویروس Norton شما می توانید پوشه ها و فایل های آلوده و مشکوک به ویروسی بودن را (که برنامهٔ ضد ویروس قادر به از بین بردن آنها نیست) قرنطینه کنید.

در صورتیکه شما با ویروسی جدید در هنگام اسکن به وسیلهٔ برنامهٔ ضد ویروس Norton روبرو شوید می توانید به سادگی آنها را قرنطینه کنید.

در این ایستگاه ما قصد داریم قرنطینه سازی فایل های آلوده را در برنامهٔ ضد ویروس Norton بررسی کنیم. برای این منظور در پنجرهٔ اصلی برنامه بر روی گزینهٔ Reports کلیک کنید و ...



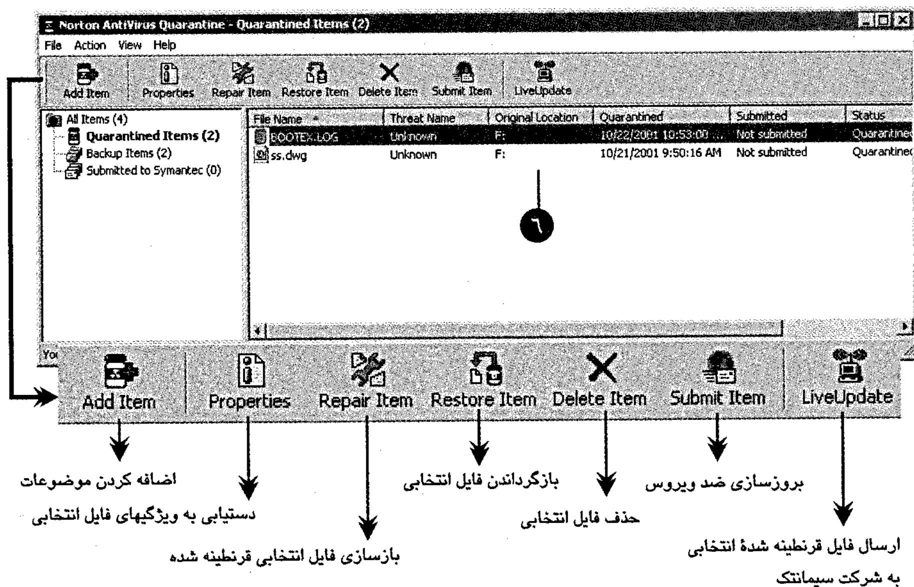
۱- گزینهٔ Reports را انتخاب کنید.

۲- گزینهٔ نمایش موضوعات قرنطینه شده را کلیک کنید.

۳- برای اضافه کردن فایل ها و پوشه ها به فضای قرنطینه، گزینهٔ Add Item را کلیک کنید.

۴- فایل مورد نظرتان را انتخاب کرده و ...

۵- کلید Add را کلیک کنید.



۶- فایل قرنطینه شده در این قسمت قابل مشاهده است.

☺ همراه: در صورتیکه شما هنگام اسکن به وسیلهٔ برنامهٔ ضد ویروس **Norton** به فایل آلوده ای برخورد کردید، با کلیک روی آیکون ارسال (Submit Item) می توانید آن را به آزمایشگاه تحقیقاتی شرکت سیمانتیک جهت بررسی هر چه بیشتر ارسال کنید.

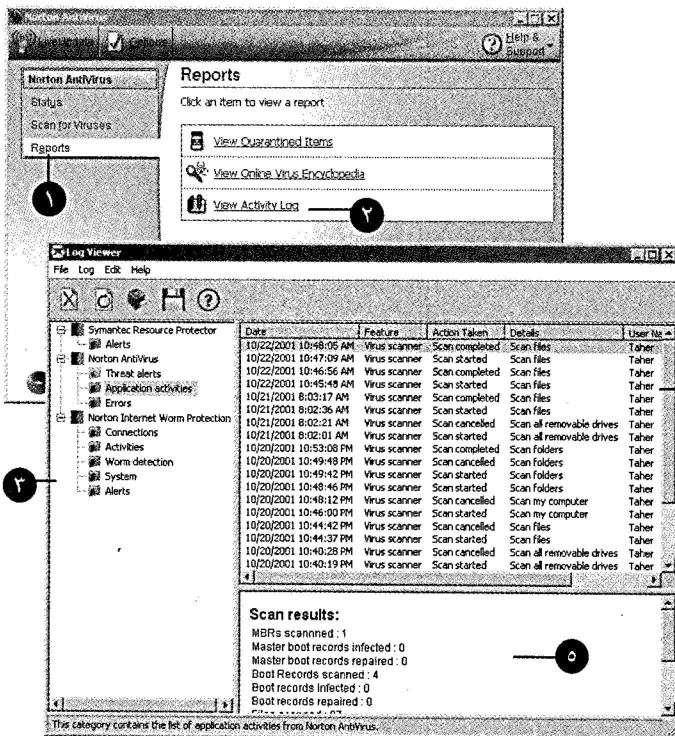
گام ششم: دیگر گزینه‌های Reports

در قسمت Reports شما دو گزینهٔ دیگر نیز مشاهده می کنید که عبارت از View Online Virus Encyclopedia (جهت مشاهدهٔ دایره المعارفی از ویروس های کامپیوتری) و دیگری View Activity Log (جهت مشاهدهٔ خلاصه گزارشی از عملکرد برنامهٔ ضد ویروس در روی کامپیوتر شما) می‌باشد.

☺ همراه: جهت مشاهدهٔ دایرهٔ المعارف ویروس ها شما باید امکانات لازم را جهت اتصال به اینترنت در کامپیوتر خود داشته باشید.

مشاهدهٔ ریز گزارش عملکرد برنامهٔ ضد ویروس

برای مشاهدهٔ ریز گزارش عملکرد برنامهٔ ضد ویروس گزینهٔ Reports را کلیک و گزینهٔ View Activity Log را انتخاب کنید و ...



۱- گزینهٔ Reports را کلیک کنید.

۲- گزینهٔ View Activity Log را انتخاب کنید.

۳- لیست عملکرد کلی ضد ویروس در این قسمت قابل مشاهده است.

۴- در این قسمت ریز اسکن های انجام شده توسط برنامه قابل مشاهده است.

۵- در این قسمت جزئیات دقیق هر اسکن را می توانید مشاهده کنید.

چاپ گرفتن از ریز عملکردهای جاری

حدف ریز عملکردهای انتخابی

راهنمایی گرفتن



بروزسازی عملکردها

ذخیره سازی ریز عملکردها

☺ بیشتر بدانیم: فرایند استفاده از ریز عملکرد با استفاده از لیست ریز عملکرد برنامهٔ ضد ویروس شما می‌توانید مدیریت بهتری را بر روی کامپیوتر و برنامهٔ ویروس یاب خود داشته باشید.

گام هفتم: به‌روزسازی برنامهٔ ضدویروس

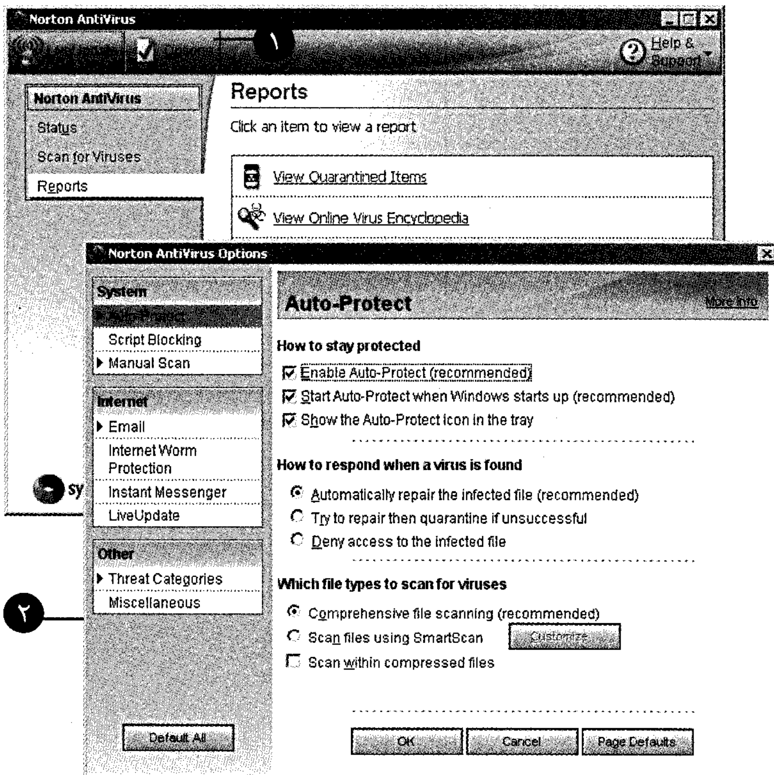
بروز سازی ضد ویروس یکی از مواردی است که هنگام استفاده از برنامه های ضد ویروس توجه خاصی را باید به آن مبذول داشت. برای انجام بروزسازی برنامهٔ ضد ویروس Norton به اینترنت متصل شده و بر روی آیکون بروزسازی در بالای پنجرهٔ اصلی برنامه کلیک کنید و ...

۱- گزینهٔ Live Update را انتخاب کنید. ۲- کلید Next را انتخاب کنید. ۳- فرایند به روزسازی در این پنجره قابل مشاهده است.

☺ همراه: رشد روز افزون انواع و اقسام ویروس ها در دنیای کامپیوتر اهمیت توجه به بروزسازی اطلاعات برنامهٔ ضد ویروس را دو چندان کرده است. خوشبختانه امروزه اکثر شرکت های بزرگ تولید کنندهٔ ضد ویروس امکانات مختلفی را جهت بروزسازی محصولات خود ارائه کرده اند.

گام هشتم: اعمال تنظیمات بیشتر بر عملکرد برنامه

در گام دوم این فصل ما با گزینه های مختلف و وضعیت موجود برنامهٔ ضد ویروس آشنا شدیم در این گام ما قصد داریم نحوهٔ اعمال تنظیمات بر روی هر یک از گزینه ها را با هم بررسی کنیم. برای اعمال تنظیمات گزینهٔ Options را در بالای پنجرهٔ اصلی انتخاب کنید و ...



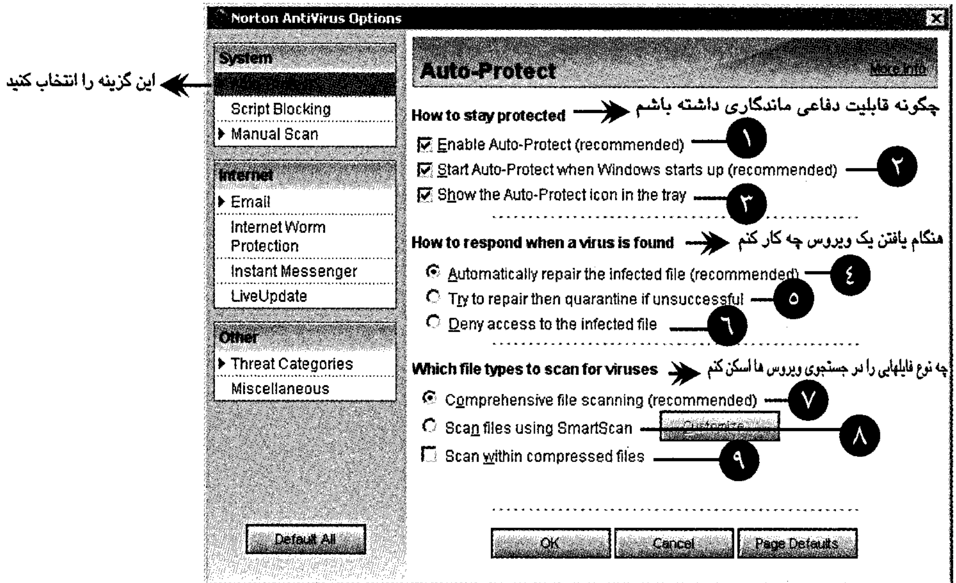
۱- گزینهٔ Options را انتخاب کنید.

۲- پنجرهٔ تنظیمات در روی صفحه نمایش ظاهر می گردد.



تنظیمات مربوط به *Auto Protect*

همانطور که اشاره شد فعال بودن این گزینه قابلیت دفاعی دائمی برنامهٔ ضد ویروس را تا حد زیادی بالا می برد. برای اعمال تنظیمات بر روی گزینهٔ Auto Protect کلیک کنید و ...



۱- با انتخاب این گزینه شما می توانید قابلیت Auto Protect را در ضد ویروس فعال کنید.

۲- با انتخاب این گزینه شما می توانید قابلیت Auto Protect را از ابتدای شروع به کار سیستم عامل ویندوز فعال کنید.

۳- با انتخاب این گزینه شما می توانید آیکون قابلیت دفاعی ضد ویروس را در کنار ساعت کامپیوتر خود مشاهده کنید.

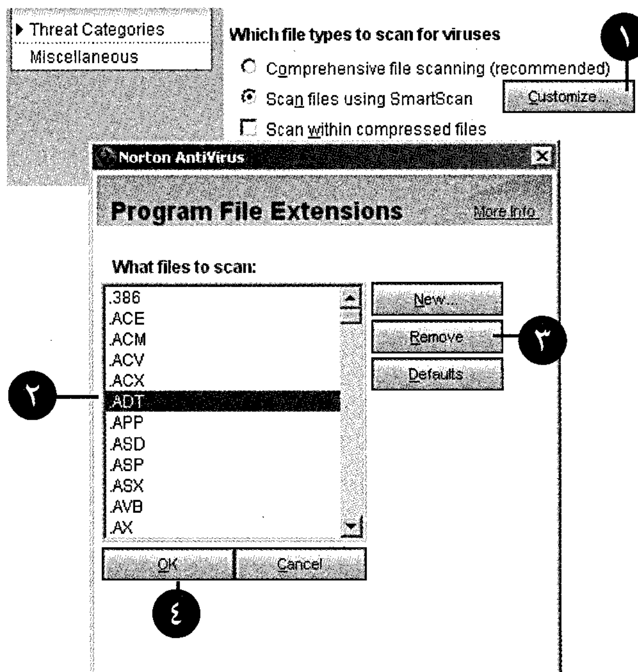
۴- با انتخاب این گزینه شما به ضد ویروس می گویید که هنگام یافتن فایل آلوده به ویروس آن را به صورت اتوماتیک بازسازی کند.

۵- با انتخاب این گزینه شما به ضد ویروس می گویید که ابتدا فایل آلوده به ویروس را بازسازی کند و در صورت عدم موفقیت آنرا قرنطینه نماید.

۶- با انتخاب این گزینه شما به ضد ویروس می گویید که از دسترسی کاربر به فایل آلوده جلوگیری کند.

۷- با انتخاب این گزینه شما به ضد ویروس می گویید که اقدام به یک اسکن فراگیر گسترده کند.

۸- با انتخاب این گزینه شما به ضد ویروس می گویید که بر اساس یک لیست سفارشی اقدام به اسکن فایل هایی خاص کند. به محض انتخاب این گزینه کلید Customize فعال می شود.



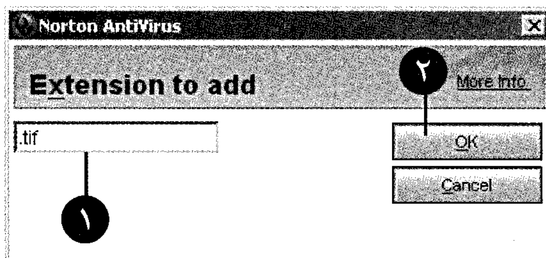
۱- این کلید را کلیک کنید.

۲- فرمت فایل مورد نظرتان را از این لیست انتخاب کنید.

۳- کلید Remove را جهت حذف فرمت مورد نظرتان از لیست ویروس یابی کلیک کنید.

۴- جهت تأیید، کلید OK را کلیک کنید.

☺ همراه: جهت اضافه کردن فرمتی خاص به لیست اسکن کلید New را کلیک کرده و ...



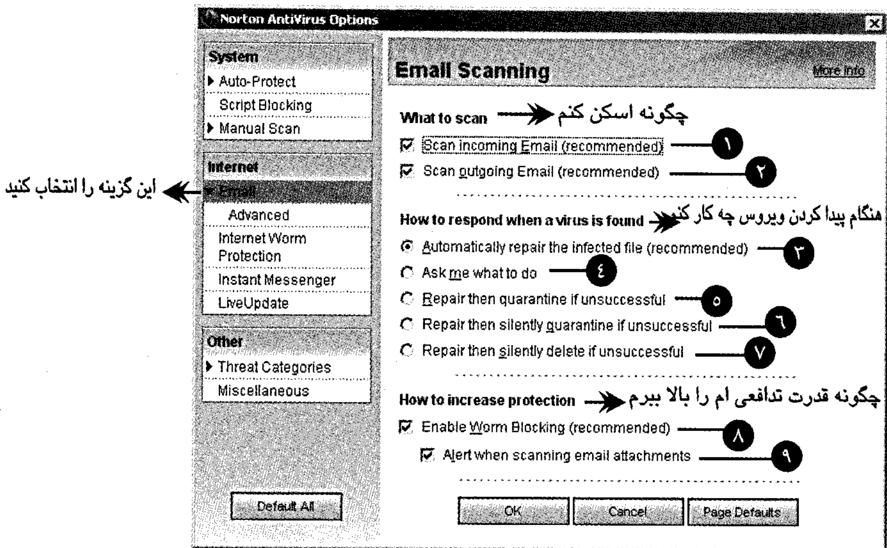
۱- فرمت مورد نظرتان را در این کادر تایپ کنید.

۲- کلید OK را کلیک کنید.

۹- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که حتی فایل های فشرده شده را هم اسکن کند.

تنظیمات مربوط به *Email Scanning*

همانطور که شما می دانید یکی از شایع ترین روش های گسترش و پراکندگی برنامه های ضد ویروس از طریق ایمیل ها می باشند. از این رو بررسی دقیق ایمیل های دریافتی یکی از وظایف مهم برنامه های ضد ویروس می باشد که توجه خاصی را باید به آن مبذول کرد. برای تنظیم گزینه های مربوط به Emailها، گزینهٔ Email را انتخاب کرده و ...



۱- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که ایمیل های ارسالی را اسکن کند.

۲- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که ایمیل های دریافتی را اسکن کند.

۳- با انتخاب این گزینه، شما به برنامهٔ ضد ویروس می گویید که پس از پیدا کردن ویروس، اقدام به بازسازی فایل آلوده کند.

۴- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که از کاربر کسب تکلیف کند.

۵- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که ابتدا فایل آلوده به ویروس را بازسازی کند و در صورت عدم موفقیت آنرا قرنطینه کند.

۶- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که ابتدا فایل آلوده به ویروس را بازسازی کند و در صورت عدم موفقیت کم کم آنرا قرنطینه کند.

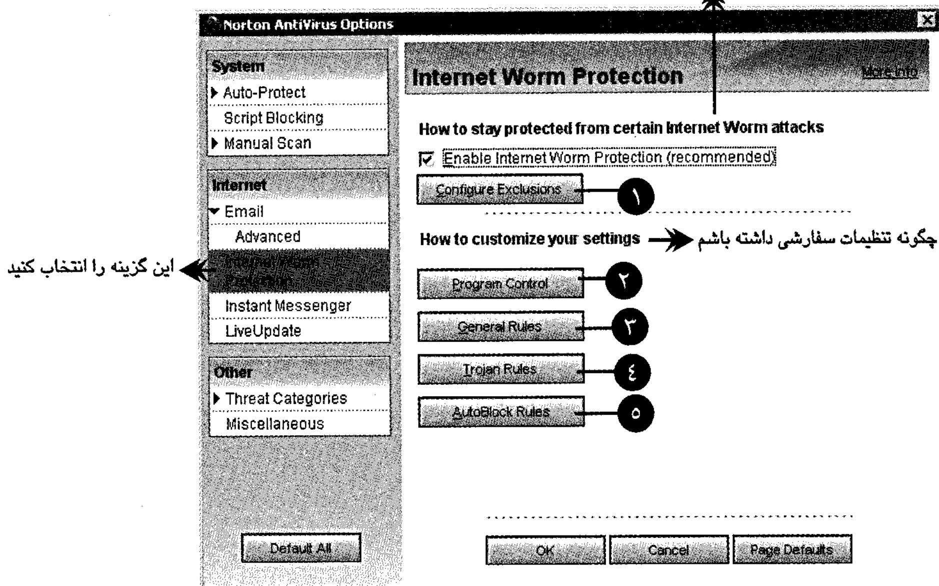
۷- با انتخاب این گزینه شما به برنامهٔ ضد ویروس می گویید که ابتدا فایل آلوده به ویروس را بازسازی کند و در صورت عدم موفقیت آن را حذف کند.

۸- با انتخاب این گزینه شما کرم های اینترنتی را بلوکه می کنید.

۹- با انتخاب این گزینه هنگام اسکن پیوست یک ایمیل، علامتی داده می شود.

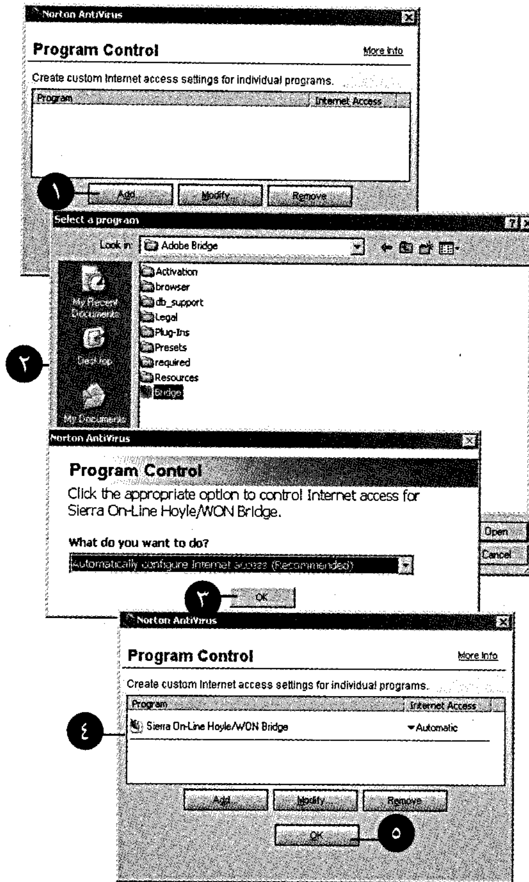
تنظیمات مربوط به *Internet Worm Protection*

یکی از گزینه های ضد ویروس Norton گزینهٔ Internet Worm Protection می باشد که امکان مقابله با کرم های اینترنتی را برای کامپیوتر شما فراهم می کند. برای اعمال تنظیمات مورد نظرتان بر روی این قابلیت ضد ویروس، گزینهٔ Internet Worm Protection را در پنجرهٔ تنظیمات انتخاب کنید و ...



۱- با کلیک کردن روی این کلید پنجره ای به نام Signature Exclusions در روی صفحه باز می شود و شما می توانید وضعیت مقابله با کرم ها را پیکربندی کنید.

۲- با کلیک کردن روی این کلید در پنجرهٔ باز شده می توانید کنترل مناسبی را بر روی برنامه ای خاص (در اینترنت) اعمال کنید.



۱- برای اضافه کردن کلید Add را کلیک کنید.

۲- برنامهٔ مورد نظرتان را انتخاب کرده و کلید Open را کلیک کنید.

۳- کلید OK را کلیک کنید.

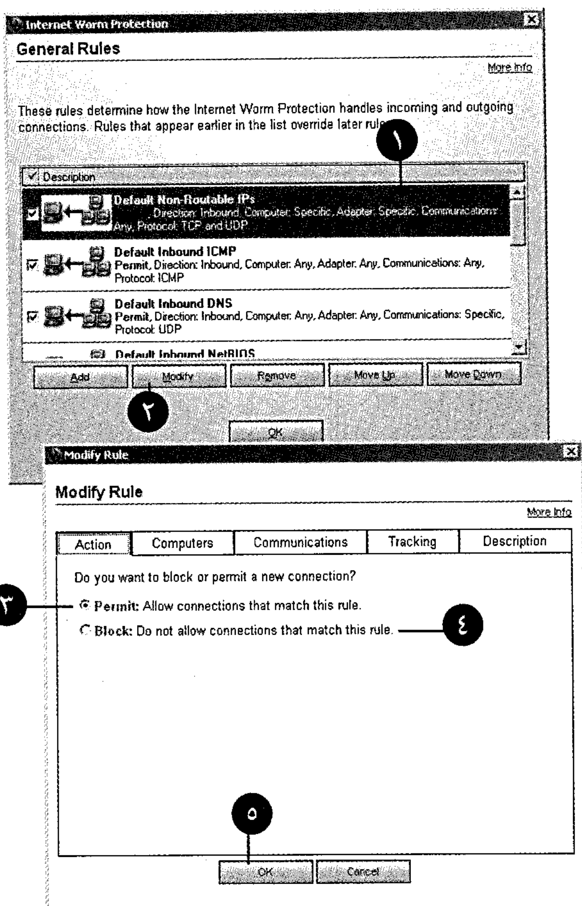
۴- حالا برنامه در این لیست قابل مشاهده است.

۵- کلید OK را جهت اتمام فرایند، کلیک کنید.

☺ **همراه:** جهت برداشتن نام برنامه از لیست کنترل، نام برنامه را انتخاب کرده و کلید **Remove** را در پایین پنجره انتخاب کنید.

۳- با کلیک کردن روی این کلید در پنجرهٔ باز شده شما می توانید نگاهی به مجموعه قوانین رایج برنامه داشته باشید. این قوانین تعیین کنندهٔ نحوهٔ ورود کرم های اینترنتی به اتصالات می باشد.





۱- قانون مورد نظرتان را انتخاب کنید.

۲- کلید **Modify** را انتخاب کنید.

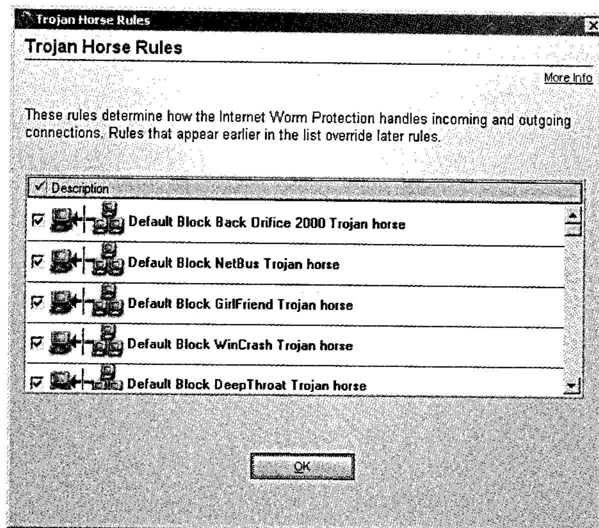
۳- با انتخاب این گزینه شما اجازهٔ اعمال قانون فوق را می دهید.

۴- با انتخاب این گزینه از اعمال قانوق فوق بر ارتباط شما جلوگیری می شود.

۵- پس از اعمال تنظیمات مورد نظرتان کلید **OK** را انتخاب کنید.

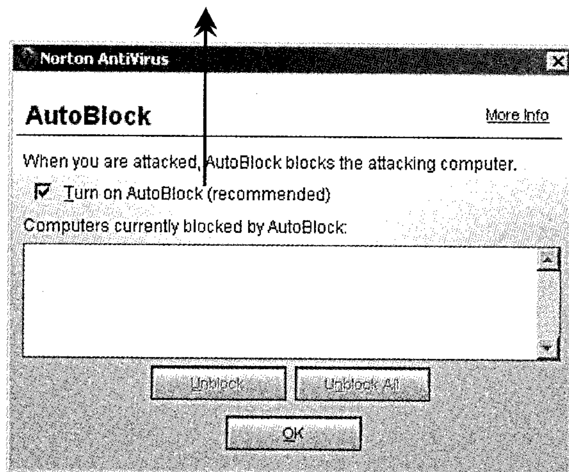
☺ همراه: گزینه های موجود در پنجره های مختلف ضد ویروس **Norton** به حدی زیاد است که می توان به هر قسمت بخش خاصی را اختصاص داد. امیدواریم در آیندهٔ نه چندان دور بتوانیم کتابی جامع در مورد این برنامهٔ جالب ارائه دهیم.

۴- با کلیک کردن روی این کلید در پنجرهٔ باز شده شما می توانید مجموعه قوانین مربوط به اسب‌های ترویا را مشاهده کنید. این مجموعه قوانین شامل آخرین روش های مقابله با اسب های ترویا می باشد.



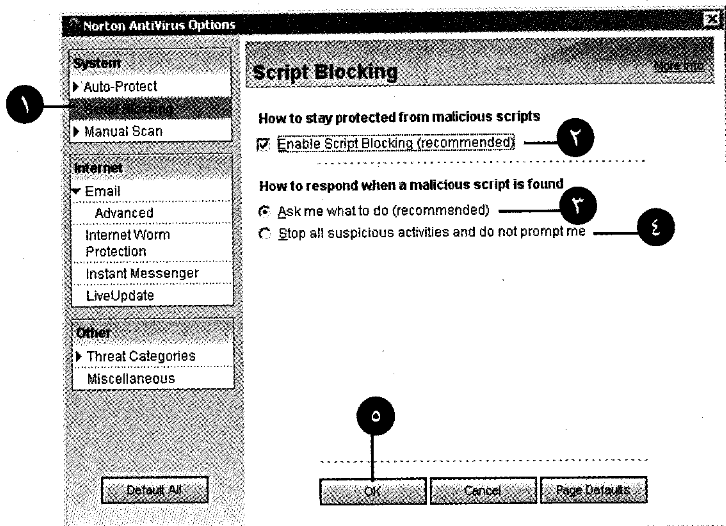
شما به سادگی می توانید هر کدام از این قوانین را غیر فعال کنید.

۵- با کلیک کردن روی این کلید شما می توانید قابلیت بلوکه کردن اتوماتیک را جهت مقابله با کرم های اینترنتی فعال کنید.



تنظیمات مربوط به *Script Blocking*

یکی از گزینه های جالب در برنامهٔ ضد ویروس Norton که در پنجرهٔ تنظیمات قابل دسترس می‌باشد Script Blocking می باشد. این گزینه امکان مقابله با عملکردهای مشکوک اسکریپت[1] ها را توسط برنامهٔ ضد ویروس به کاربر می دهد. برای اعمال تنظیمات مورد نظرتان بر روی این قابلیت، گزینهٔ Options را انتخاب کرده و در پنجرهٔ باز شده Script Blocking را انتخاب کنید.



۱- این گزینه را انتخاب کنید.

۲- گزینهٔ فعال کنندهٔ اسکریپت

۳- کسب تکلیف هنگام روبرویی با یک اسکریپت مشکوک

۴- متوقف سازی اسکریپت به صورت خودکار

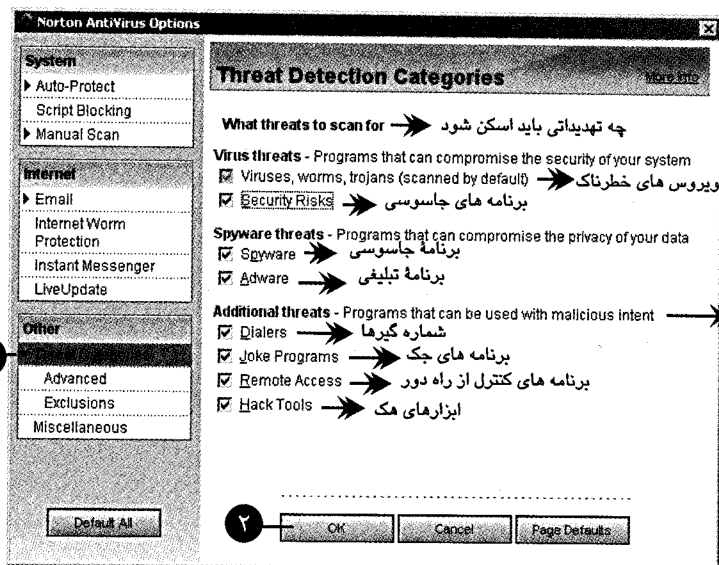
۵- پس از اعمال تنظیمات کلید OK را کلیک کنید.

تنظیمات مربوط به *Threat Detection Categories*

با استفاده از این گزینه می توانید از دستیابی به خطرات توسط برنامهٔ ضد ویروس Norton حداکثر بهره را جهت اعمال تنظیمات مورد نظرتان ببرید. برای این منظور بر روی گزینهٔ Threat Categories کلیک کنید و ...

---

[1] فایل هایی هستند که حاوی فرمان های اجرایی مثل استفاده از پست الکترونیکی می باشند.



۱- این گزینه را کلیک کنید.

۲- بعد از اعمال تنظیمات مورد نظرتان کلید OK را کلیک کنید.

☺ همراه: دیگر تنظیمات موجود در پنجرهٔ **Norton Antivirus Options** دارای گزینه های مشابه با تنظیمات ذکر شده می باشند از این رو از ذکر آنها در این کتاب خودداری می کنیم.

☺ بیشتر بدانیم: در صورتی که پس از اعمال تنظیمات انجام شده به جای کلمهٔ **On** کلمهٔ **Error** در مقابل گزینهٔ تنظیم شده ظاهر شد بهتر است یک بار کامپیوتر خود را خاموش/ روشن کنید.

خلاصهٔ این فصل

ما در این فصل با قابلیت های مختلف برنامهٔ ضد ویروس Norton آشنا شدیم و به بررسی دقیق آن پرداختیم. از توانایی های کسب شده در این فصل می توان به آشنایی با پنجرهٔ اصلی ضد ویروس، بررسی وضعیت جاری ضد ویروس، انجام ویروس زدایی و قرنطینه کردن فایل آلوده اشاره کرد. ضد ویروس Norton برنامهٔ بسیار وسیعی است که ما به اندازهٔ توان خود در این فصل به آن اشاره کردیم. مطمئناً شما قابلیت های زیادی را در این برنامه با کوشش و تلاش خود کشف خواهید کرد.

سئوالات تستی

گزینهٔ Auto Protect در پنجرهٔ اصلی برنامه چه قابلیتی را به کاربران ارائه می کند؟

الف: مقابلهٔ دائم با ویروس ها
ب: بالا بردن امنیت دائمی
پ: ویروس یابی پیوست E-mail
ج: گزینه های الف و ب

چگونه می توان به آخرین وضعیت بهنگام سازی اطلاعات ضد ویروس دست یافت؟

الف: گزینهٔ Renewal Date
ب: گزینهٔ Virus Definitions
پ: گزینهٔ Information
ج: گزینهٔ Update

گزینهٔ Scan file در پنجرهٔ ویروس یابی چه قابلیتی را به کاربران ارائه می دهد؟

الف: قابلیت اسکن پوشه ها
ب: قابلیت اسکن فایلی خاص
پ: قابلیت اسکن فلاپی دیسک
ج: هیچکدام

مزیت بزرگ زمان بندی اتوماتیک جهت اسکن برنامهٔ ضد ویروس چیست؟

الف: صرفه جویی در وقت و هزینه
ب: بالا بردن راندمان کار
پ: بالا بردن امنیت سیستم
ج: هر سه مورد صحیح است

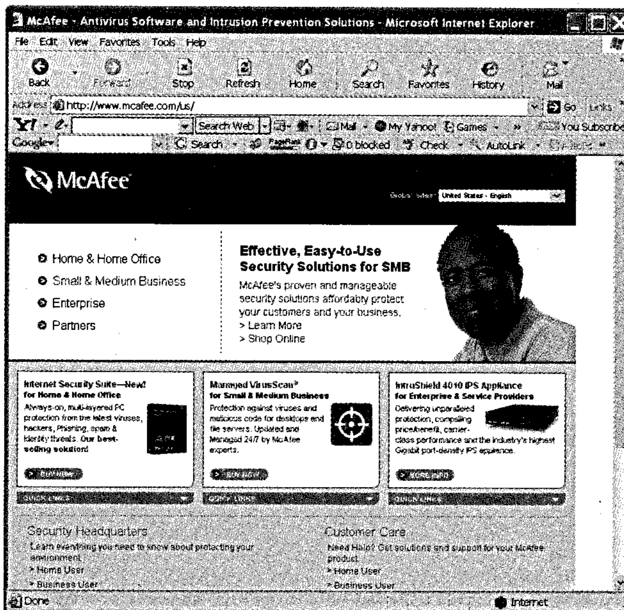
چگونه می توان آیکون ضد ویروس را در هنگام فعال شدن از کنار ساعت کامپیوتر فعال یا غیر فعال کرد؟

الف: با راست کلیک کردن و انتخاب گزینهٔ Disable
ب: با تغییر اندازهٔ صفحهٔ رومیزی
پ: با استفاده از گزینهٔ Auto-Protect در پنجرهٔ Options
ج: هیچکدام

فصل ۱۱

برنامهٔ ضدویروس McAfee

یکی از کاربردی ترین و پر استفاده ترین برنامه های ضـد ویـروس دنیـا برنامـهٔ McAfee محـصـول شرکت Network Associates می باشد. این برنامـهٔ قدرتمنـد بـه زبـان هـای مختلفـی مثـل انگلیـسی، فرانسوی، آلمانی، ایتالیایی و اسپانیایی قابل دسترس می باشد. در این بخش مـا قـصد داریـم نحـوهٔ استفاده از این برنامهٔ ضد ویروس را بررسی کنیم.



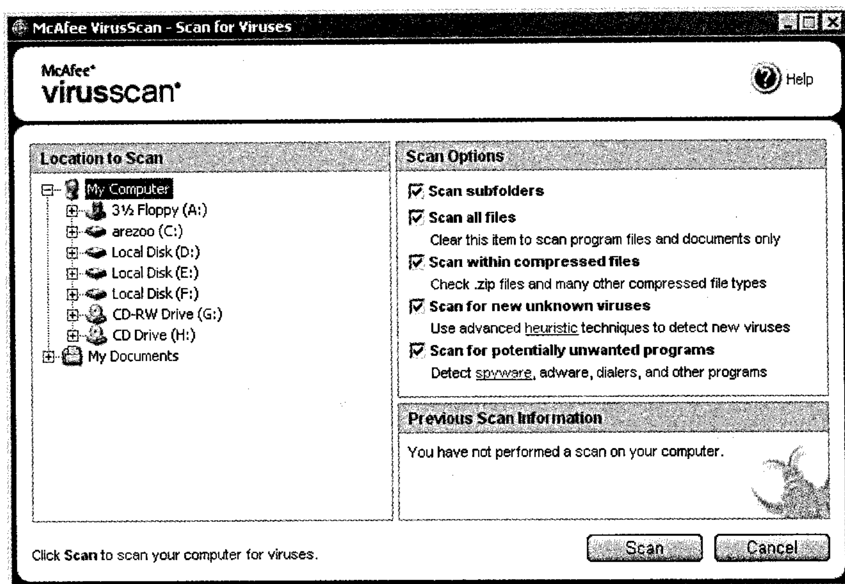


گام اول: فعال‌سازی برنامهٔ ضدویروس McAfee

در اولین ایستگاه آشنایی با برنامهٔ ضد ویروس McAfee ما قصد داریم با این برنامهٔ جذاب شروع به ویروس یابی کرده و کامپیوتر خود را پاکسازی کنیم. پس با گام های مصمم خود ما را همراهی کنید.

۱- *باز کردن پنجرهٔ اصلی برنامه*

برای باز کردن پنجرهٔ برنامهٔ McAfee، بر روی آیکون برنامه ( ) در صفحهٔ رومیزی کلیک کنید تا پنجره ای به شکل زیر در روی صفحهٔ نمایش ظاهر گردد.



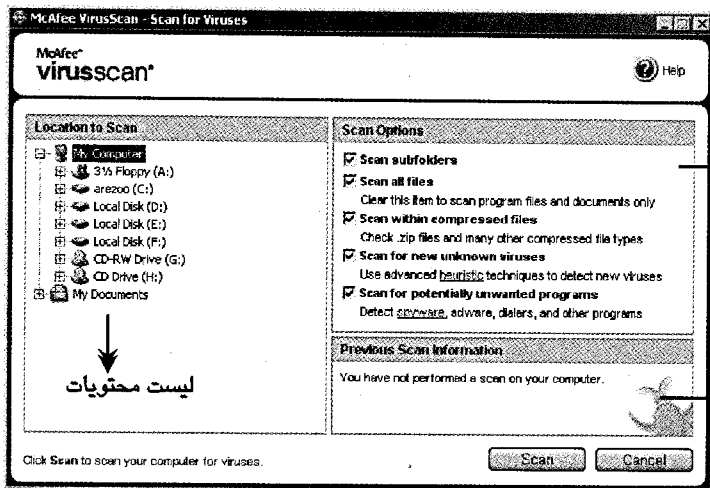
۲- *قسمتهای مختلف پنجره*

همانطور که مشاهده می کنید پنجرهٔ ضد ویروس McAfee شامل سه قسمت به شرح زیر می باشد:

☑ **لیست محتویات:** از این لیست شما می توانید درایو، فایل و پوشهٔ مورد نظرتان را جهت اسکن ویروس ها انتخاب کنید.

☑ **کادر گزینه ها:** از این قسمت شما می توانید تنظیماتی را برای انجام اسکن برنامهٔ ضد ویروس فعال یا غیر فعال کنید.

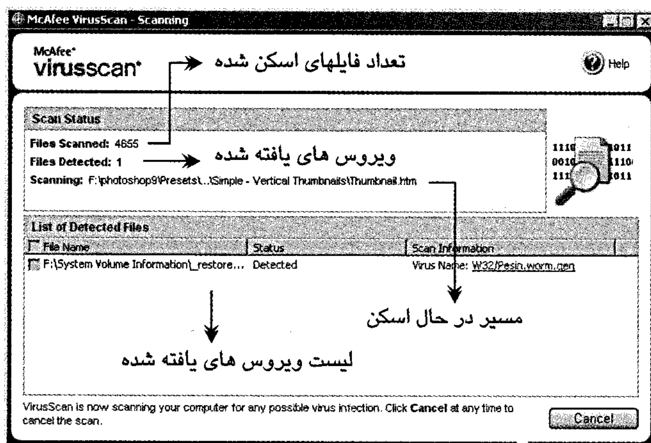
☑ **کادر اطلاعات:** از این قسمت شما می توانید به اطلاعات مختلفی مثل تاریخ آخرین اسکن انجام شده، تعداد فایل های اسکن شده و ویروس های پیدا شده دست پیدا کنید.



☺ همراه: کلیهٔ گزینه های قابل تنظیم در کادر گزینه های به صورت پیش فرض فعال را آزمایش کنید، در ادامه این فصل به بررسی هر یک از این تنظیمات خواهیم پرداخت.

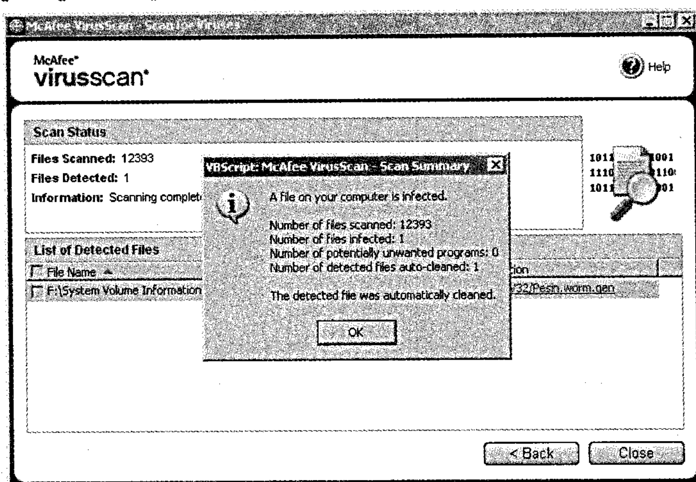
۴- شروع ویروس یابی

بعد از اینکه درایو مورد نظرتان را جهت ویروس زدایی از کادر گزینه ها انتخاب کردید کلید Scan را در پایین پنجره کلیک کنید در این حالت پنجره ای شروع فرایند اسکن درایو انتخابی را توسط برنامهٔ ضد ویروس نمایش می دهد.



۵- اتمام ویروس یابی

بعد از اتمام فرایند اسکن، در صورتیکه برنامه موفق به پیدا کردن ویروسی در درایـو انتخـابی شـما شود در لیست ویروس ها آنها را نمایش می دهد و توسط پنجره ای شناور به شما گزارش اسکن را می دهد. در کادر فوق برای پایان بخشیدن به اسکن فایل ها بر روی کلید OK کلیک کنید.



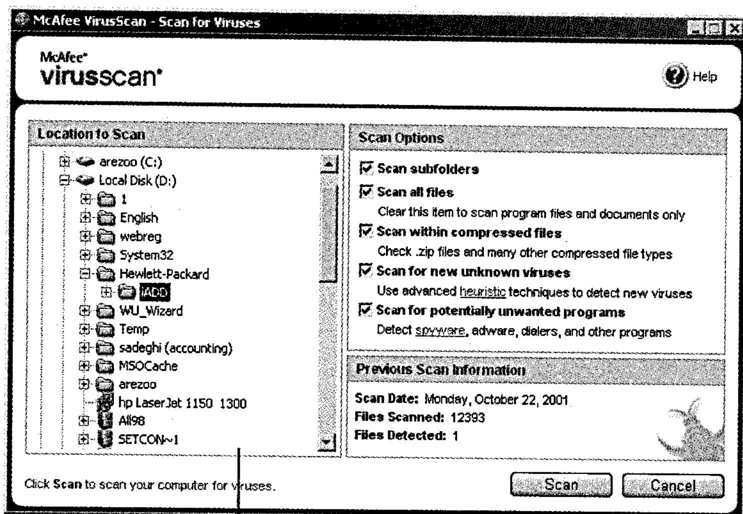
> ☺ همراه: در صورتیکه برنامهٔ McAfee موفق به پیدا کردن هیچ ویروسی بر روی کامپیوتر شما نـشود نیـز بـا نمایش پنجره ای این مسئله را به شما گزارش می دهد.

گام دوم: آشنایی بیشتر با گزینه‌های ضدویروس McAfee

در گام قبل ما به صورت کلی با فرایند اسکن و ویروس زدایی به وسیلهٔ برنامهٔ McAfee آشنا شـدیم در این گام قصد داریم بر روی این فرایند تأمل بیشتری داشته باشیم. یکی از مزایای بزرگ ویـروس یابی به وسیلهٔ برنامهٔ McAfee عدم نیاز به هیچ مایع ضد عفونی، ماسـک و روپـوش اسـت. شـما بـا خیال راحت می توانید از این برنامهٔ جالب به بهترین نحو ممکن بهره ببرید.

۱- انتخاب دقیق

جهت انتخاب پوشه، فایل، درایو یا حتی کل محتویات کامپیوتر، شما می توانید از لیست محتویـات در پنجرهٔ اصلی برنامهٔ McAfee استفاده کنید. برای انتخاب یک پوشه یا فایل بر روی علامت بعـلاوه (+) سمت چپ هر درایو کلیک کرده و روی فایل و پوشهٔ مورد نظرتان کلیک کنید.

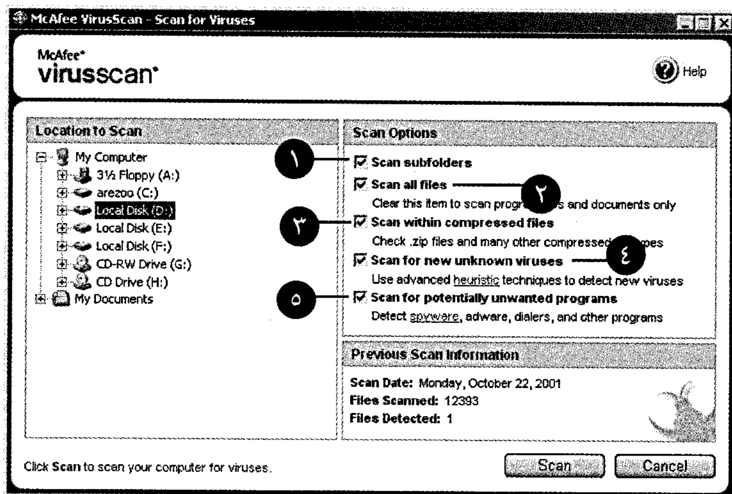


پوشه، فایل و درایو مورد نظرتان

را از این قسمت انتخاب کنید

۲- اعمال تنظیمات بیشتر

جهت اعمال تنظیمات بیشتر بر نحوهٔ عملکرد اسکن ضد ویروس McAfee شما می توانید از کادر تنظیمات در پنجرهٔ اصلی برنامه استفاده کنید. گزینه های قابل تنظیم و عملکرد آنها به شرح زیر است:



۱- **گزینهٔ Scan Subfolder**: با انتخاب این گزینه شما می توانید تمام زیر پوشه های داخل یک پوشه را نیز در جستجوی ویروس ها اسکن کنید.

۲- **گزینهٔ Scan all files**: با انتخاب این گزینه شما می توانید تمام پوشه های درایو یا پوشهٔ انتخابی را اسکن کنید.

۳- **گزینهٔ Scan within compressed file**: با انتخاب این گزینه شما می توانید تمام پوشه هـای zip و فشرده شده را اسکن کنید.

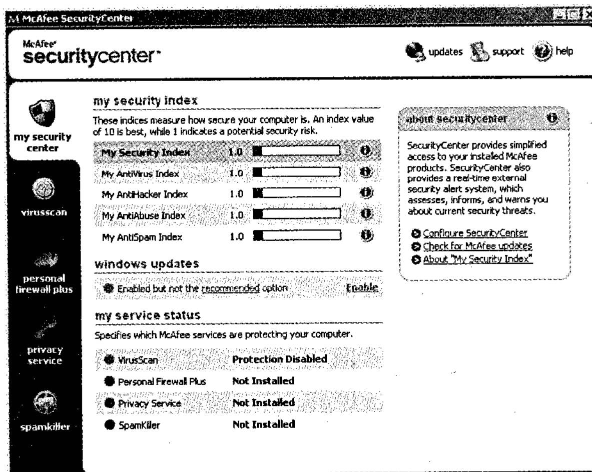
۴- **گزینهٔ Scan for potentially unwanted programs**: با انتخاب این گزینـه شـما مـی توانیـد بـه اسکن و ویروس زدایی برنامه های مـشکوک بـه ویروسـی بـودن بپردازیـد. ایـن برنامـه هـا شـامل برنامه‌های جاسوسی، برنامه های تبلیغاتی و برنامه های شماره گیر می باشد.

گام سوم: تنظیم فعال‌سازی اتوماتیک ضدویروس McAfee

همانطور که در بخش های قبلی این کتاب بـه آن اشـاره داشـتیم یکـی از راه هـای کارآمـد مقابلـه بـا ویروس های کامپیوتری استفاده از قابلیت فعال سازی اتوماتیک می باشد. در این ایـستگاه مـا قـصد داریم نحوهٔ فعال سازی اتوماتیک برنامهٔ McAfee را بررسی کنیم.

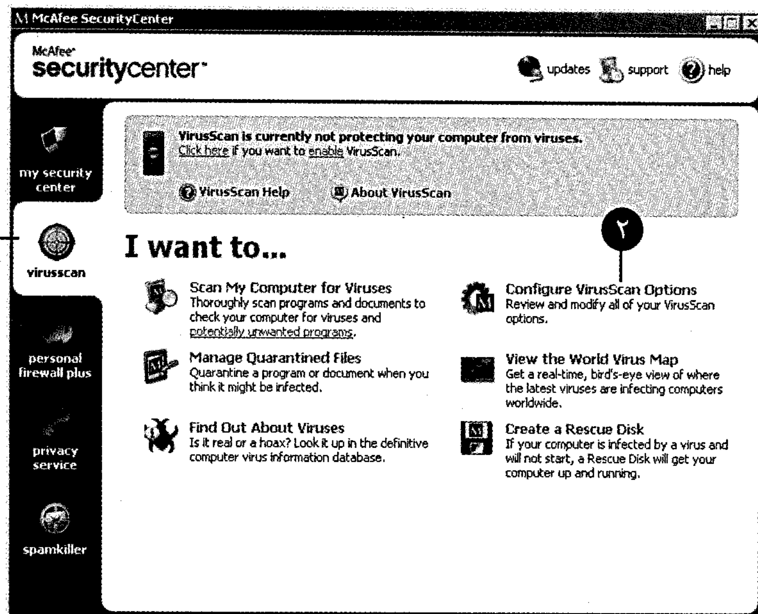
۱- پنجرهٔ *Security Center*

بر روی آیکون McAfee Security (M) در روی صفحهٔ رومیزی کامپیوتر یا کنار ساعت کلیک کنید تا پنجره ای به شکل زیر در روی صفحه نمایش ظاهر گردد.



۲- عنوان *Virus Scan*

در پنجرهٔ فوق بر روی لبهٔ کناری پنجره، بر روی عنوان Virus scan کلیک کرده و از بین گزینه هـای موجود، گزینهٔ Configure Virus Scan Options را انتخاب کنید.



۱- این عنوان را انتخاب کنید.

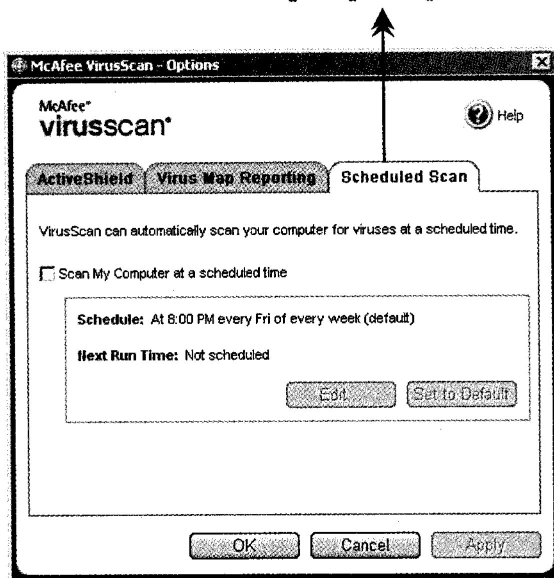
۲- این گزینه را انتخاب کنید.

۳- پنجرهٔ *Options*

در این حالت پنجره ای به نام McAfee Virus Scan-Option در روی صفحهٔ نمایش ظاهر می شـود. برای مشاهدهٔ پارامترهای مربوط به فعال سازی اتوماتیک عنوان Scheduled Scan را انتخاب کنید.



این عنوان را برای مشاهدهٔ
تنظیمات کلیک کنید



۴- تنظیم زمان اسکن اتوماتیک

برنامهٔ McAfee بصورت پیش فرض در ساعت ۸ بعد از ظهر هر هفته اقدام به اسکن محتویات کامپیوتر می کند. جهت تنظیم زمان اسکن به صورت دلخواه گزینهٔ ... Scan My Computer at را انتخاب و کلید Edit را کلیک کنید.

۱- این گزینه را انتخاب کنید.

۲- این کلید را انتخاب کنید.

۳- زمان اسکن را از این منوی کشویی انتخاب کنید.

۴- ساعت دقیق اسکن را در این کادر وارد کنید.

۵- تعداد دفعات تکرار اسکن را در این کادر وارد کنید.

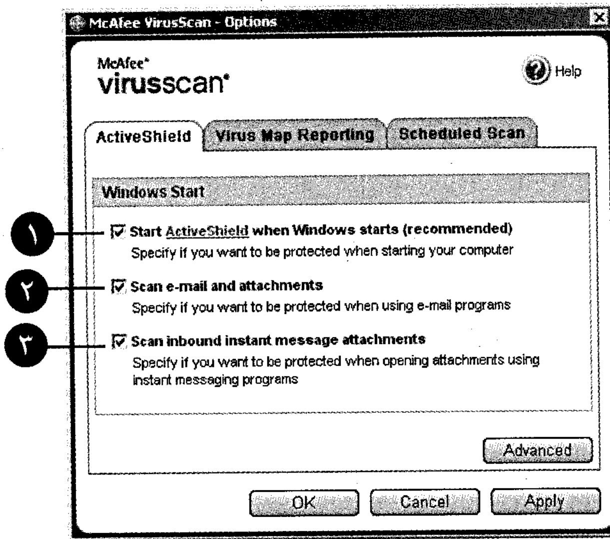
۶- روز اسکن را از بین این گزینه ها انتخاب کنید.

۷- کلید OK را کلیک کنید.



۵- زمان فعال سازی سپر دفاعی

برای تنظیم زمان فعال سازی سپر دفاعی برنامهٔ ضد ویروس McAfee عنوان Active Shield را در پنجرهٔ MacAfee Virus Scan-Option انتخاب کنید.



پنجرهٔ فوق شامل سه گزینه به شرح زیر می باشد:

۱- **گزینهٔ Start Active Shield**: با انتخاب این گزینهٔ سپر دفاعی برنامهٔ ضد ویروس در هنگام فعال شدن ویندوز فعال می شود.

۲- **گزینهٔ Scan E-mail and attachment**: با انتخاب این گزینه برنامهٔ ضد ویروس، فایل های پیوستی E-mail ها را نیز اسکن می کند.

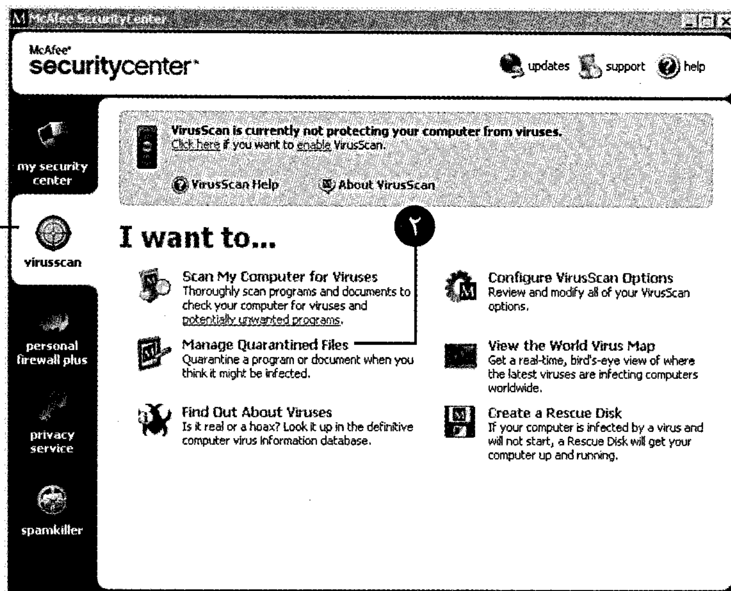
۳- **گزینهٔ ... Scan inbound instant message**: با انتخاب این گزینه فایل های پیوستی E-mail ها به صورت آنی اسکن می گردد.

گام چهارم: قرنطینه کردن فایل‌های آلوده

همانطور که قبلاً به آن اشاره شد در دنیای بزرگ کامپیوتر شما هر روز میزبان یک ویروس با ویژگی های خاص و منحصر به فرد می باشید. از این رو شما برای مقابلهٔ هر چه بهتر با این ویروس های جدید باید برنامهٔ ضد ویروس خود را به روز کنید.
هنگام اسکن کردن محتویات کامپیوتر خود به وسیلهٔ ضد ویروس McAfee ممکن است شما با تعدادی از این ویروس ها برخورد کنید. برنامهٔ ضد ویروس McAfee خوشبختانه قابلیت شناسایی

این ویروس ها را دارد و اسامی فایل های آلوده به این ویروس ها را به شما اعلام می کند. شما به وسیلهٔ قابلیت قرنطینه کردن می توانید این فایل های آلوده را برای تصمیم گیری آتی و عدم آلوده سازی فایل های دیگر بلوکه کنید.

برای این منظور پنجرهٔ McAfee Security Center را باز کرده و عنوان Virus scan را کلیک کنید تا تنظیمات مربوطه در پنجرهٔ فوق قابل مشاهده شود.

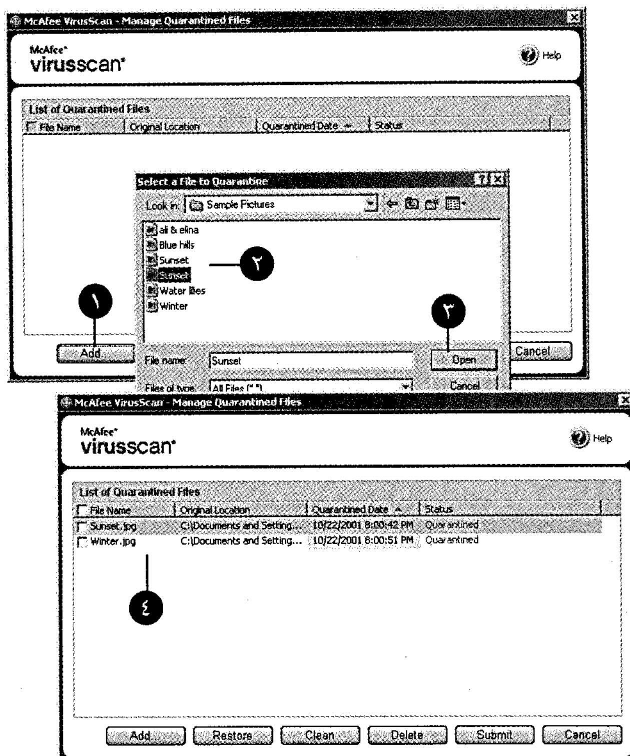


۱- این گزینه را انتخاب کنید.

۲- این گزینه را انتخاب کنید.

برای باز شدن پنجرهٔ مدیریت قرنطینه گزینهٔ Manage Quarantined File را کلیک کنید. با کلیک کردن روی کلید Add شما می توانید فایل های مورد نظرتان را به پنجرهٔ قرنطینه اضافه نمایید.





۱- کلید Add را برای اضافه کردن فایل های مورد نظرتان انتخاب کنید.

۲- فایل های مورد نظرتان را جهت قرنطینه کردن، این این پنجره انتخاب کنید.

۳- کلید Open را کلیک کنید.

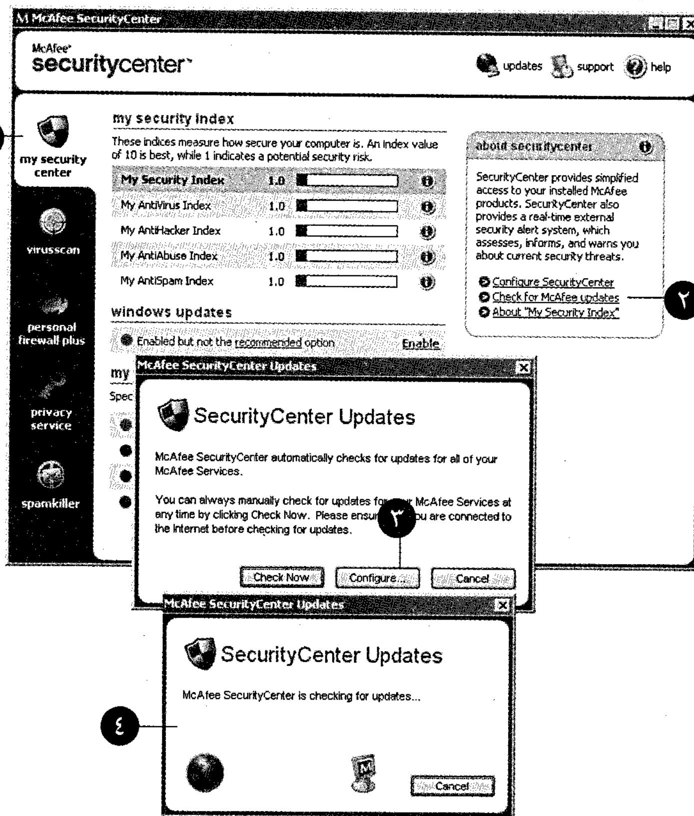
۴- فایل های تحت قرنطینه در این قسمت قابل مشاهده است.

☺ همراه: برای حذف فایل تحت قرنطینه شما کافی است کنار فایل مورد نظرتان کلیک کنید تا علامت چک (✓) در کنار آن ظاهر گردد و سپس کلید **Delete** را کلیک کنید.

گام پنجم: به‌روزسازی برنامهٔ ضد ویروس McAfee

یکی از عوامل مهم در بالا بردن قدرت دفاعی برنامهٔ ضد ویروس در مقابل ویروس ها به روز سازی منظم و دقیق برنامه می باشد. به وسیلهٔ به روز سازی شما می توانید آخرین اطلاعات مربوط به ویروس و روش مقابله با آنها را به ضد ویروس خود اضافه کنید.

برای این منظور پنجرهٔ McAfee Security Center را باز کرده و در پنجرهٔ فوق عنوان My Security Center را کلیک کنید.



۱- این عنوان را انتخاب کنید.

۲- گزینهٔ فوق را انتخاب کنید.

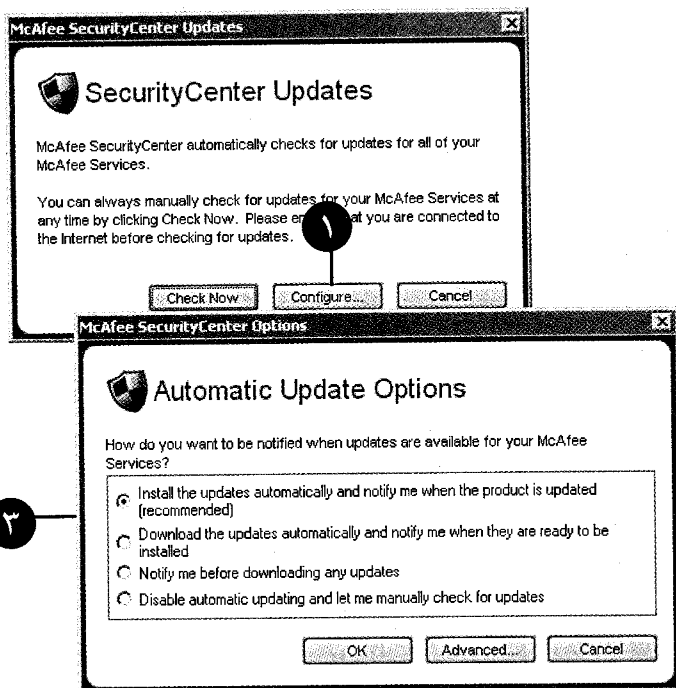
۳- گزینهٔ Check Now را انتخاب کنید.

۴- روند به روزسازی ضد ویروس، در این پنجره قابل مشاهده است.

☺ همراه: قبل از انتخاب گزینهٔ Check Now حتماً به اینترنت متصل شوید.

پیکربندی بروزسازی

جهت پیکربندی و تنظیم به روزسازی برنامهٔ ضد ویروس McAfee، کلید Configure را در پنجرهٔ McAfee Security Center Updates کلیک کنید.



۱- کلید **Configure** را کلیک کنید.

۲- در این پنجره شما می توانید تنظیمات مربوط به پیکربندی ضد ویروس را انجام دهید.

پنجرهٔ پیکربندی شامل چهار گزینه به شرح زیر می باشد:

☑ **...Install the updates**: با انتخاب این گزینه عملیات به روزسازی ضد ویروس به صورت اتوماتیک انجام شده و اتمام فرایند به روزسازی به شما اطلاع داده می شود.

☑ **...Download the updates**: با انتخاب این گزینه به محض نیاز به بروزسازی برنامهٔ ضد ویروس این کار به صورت اتوماتیک انجام می گیرد.

☑ **...Notify me before**: با انتخاب این گزینه قبل از هر اقدام به شما اطلاع داده می شود.

☑ **... Diable automatic updating**: با انتخاب این گزینه قابلیت به روزسازی اتوماتیک برنامهٔ ضد ویروس غیر فعال می گردد.

تنظیم گزینه های هوشیار باش

برنامهٔ ضد ویروس McAfee جهت ارائهٔ اخطار و آگاهی به کاربران از امکانات مختلفی مثل یک کادر پیغام یا یک آهنگ اخطار کوتاه استفاده می کند. برای تنظیم نوع و شکل اخطار شما کافی است در پنجرهٔ McAfee Security Center کلید Configure Security Center را انتخاب کنید.

McAfee SecurityCenter Updates

SecurityCenter Updates

McAfee SecurityCenter automatically checks for updates for all of your McAfee Services.

You can always manually check for updates for your McAfee Services at any time by clicking Check Now. Please ensure that you are connected to the Internet before checking for updates.

۱

Check Now | Configure... | Cancel

McAfee SecurityCenter Options

Automatic Update Options

How do you want to be notified when updates are available for your McAfee Services?

- Install the updates automatically and notify me when the product is updated (recommended)
- Download the updates automatically and notify me when they are ready to be installed
- Notify me before downloading any updates
- Disable automatic updating and let me manually check for updates

۲

OK | Advanced... | Cancel

McAfee SecurityCenter Options

Advanced Alert Options

What kind of Security Alerts would you like to see?

- Display all virus outbreak and other security alerts (recommended)
- Do not display any security alerts

۳

Would you like to hear a sound when an alert is displayed?

- Play a sound when a security alert is displayed
- Play a sound when a product update alert is displayed

٤

OK | Cancel

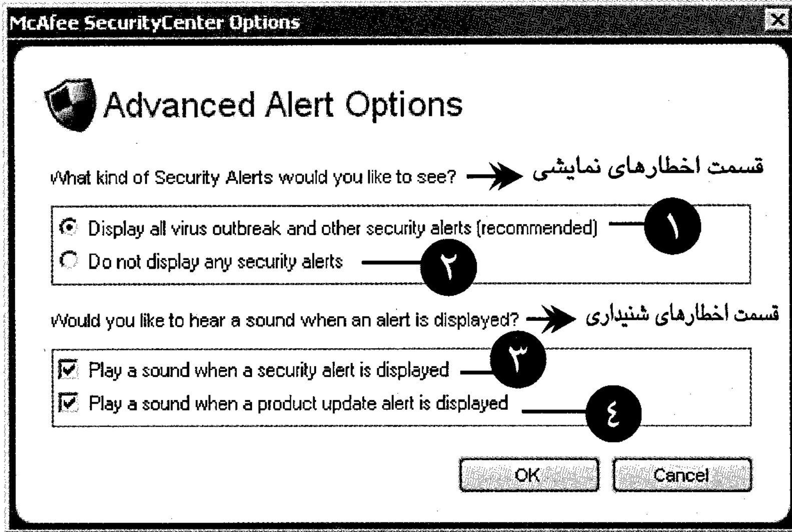
۱- این گزینه را کلیک کنید.

۲- کلید Advanced را انتخاب کنید.

۳- تنظیمات مورد نظرتان را برای نوع اخطار در این پنجره انجام دهید.

۴- کلید OK را انتخاب کنید.

پنجرهٔ فوق دارای دو قسمت به شرح زیر می باشد:



۱- با انتخاب این گزینه هنگام پیدا کردن ویروس یا برخورد با مشکلات امنیتی پنجرهٔ اخطار در روی صفحهٔ نمایش ظاهر می شود.

۲- با انتخاب این گزینه هیچ پنجره ای در روی صفحه نمایش ظاهر نمی شود.

۳- با انتخاب این گزینه در صورت پیدا کردن ویروس به وسیلهٔ برنامهٔ ضد ویروس اخطاری به صورت آهنگ پخش می شود.

۴- با انتخاب این گزینه جهت به روزسازی آهنگی به صورت اخطار ظاهر می شود.

☺ همراه: استفاده از قابلیت های ارائهٔ اخطار و آگهی در برنامهٔ **McAfee** یکی از ویژگی هایی است که استفاده از آن محیط لذت بخشی را برای کاربران این ضد ویروس فراهم می کند. تنظیم دقیق این اخطارها مدیریت شما را بر نحوهٔ عملکرد برنامه های ضد ویروس بالا می برد.

گام ششم: ساخت دیسک نجات

همانطور که قبلاً نیز به آن اشاره کردیم ساخت دیسکت نجات یکی از نکاتی است که نقش مهمی در بالا بردن ضریب امنیتی کامپیوتر شما بازی می کند. در این گام ما قصد داریم نحوهٔ ساخت یک دیسک نجات به وسیلهٔ ضد ویروس McAfee را بررسی کنیم.

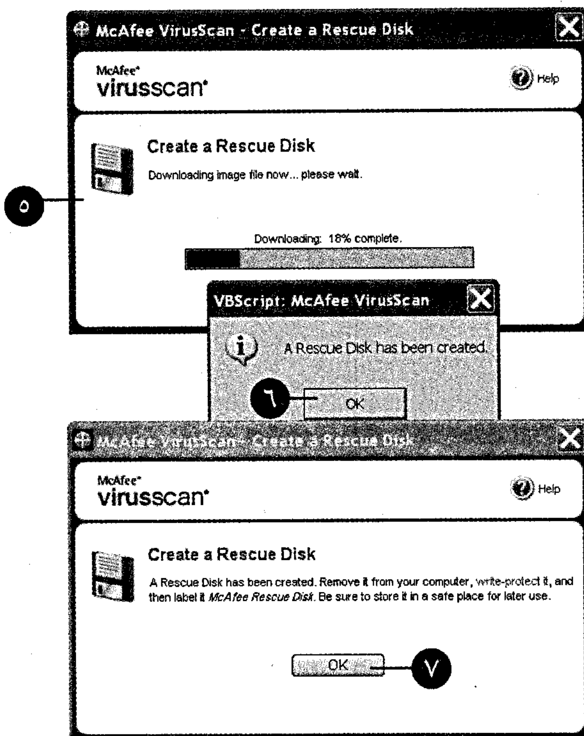
برای ساخت یک دیسک نجات ابتدا به اینترنت متصل شوید و یک فلاپی دیسک خالی را در داخل فلاپی درایو کامپیوتر خود قرار داده و گزینهٔ Virus Scan را در پنجرهٔ Security Center انتخاب کنید.

۱- عنوان Virus scan را کلیک کنید.

۲- گزینهٔ Create Rescue Disk را انتخاب کنید.

۳- کلید Create را کلیک کنید.

۴- در این حالت پنجره ای به شما اخطار می دهد که کلیهٔ محتویات قبلی فلاپی دیسک پاک می شود. کلید OK را در پنجرهٔ فوق انتخاب کنید.



۵- در پنجرهٔ فوق فرایند ساخت دیسک نجات قابل مشاهده است.

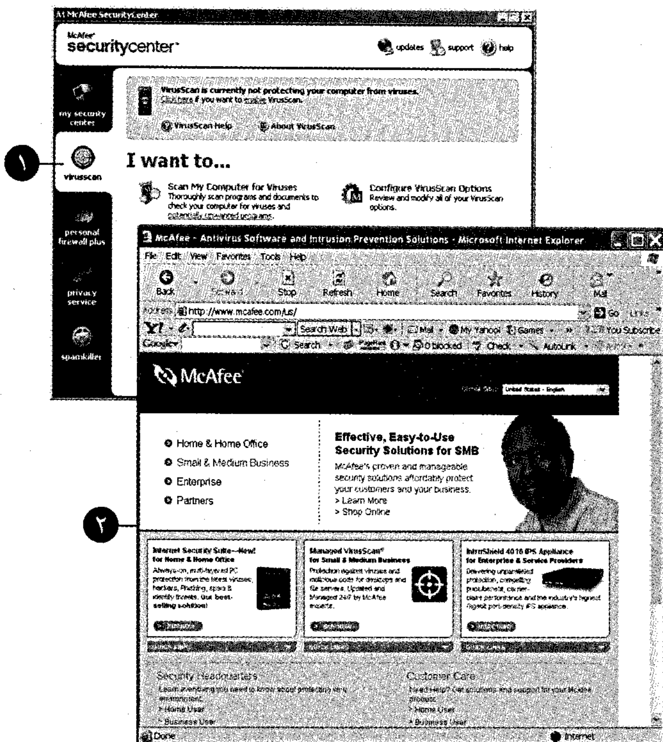
۶- پس از چند لحظه پنجره ای ساخت موفقیت آمیز دیسک نجات را به شما اعلام می کند در پنجرهٔ فوق کلید OK را انتخاب کنید.

۷- در این پنجره تذکراتی در مورد حفظ و نگهداری فلاپی ذکر شده است پس از مطالعهٔ این تذکرات کلید OK را انتخاب کنید.

☺ همراه: پس از ساخت دیسک نجات، فلاپی دیسک را از فلاپی درایو خارج کرده و از آن به دقت محافظت کنید. مطمئن باشید این دیسک در روز مبادا به نجات شما خواهد آمد.

گام هفتم: دستیابی به آخرین اطلاعات در مورد ویروس‌ها

داشتن اطلاعات در مورد آخرین ویروس های دنیا یکی از راه کارهای مهم در شناخت و مقابله با ویروس ها می باشد. برنامهٔ McAfee امکان دستیابی به آخرین اطلاعات در مورد ویروس های شایع دنیا را به سادگی برای شما فراهم می کند. برای این منظور به اینترنت متصل شوید و گزینهٔ Virus Scan را در پنجرهٔ Security Center انتخاب کنید.



۱- جهت دستیابی به آخرین اطلاعات در مورد ویروس ها این گزینه را انتخاب کنید.

۲- در این وب سایت شما می توانید به آخرین اطلاعات در مورد ویروس ها دست یابید.

مشاهدهٔ نقشهٔ پراکندگی و گسترش ویروس ها

برای مشاهدهٔ نقشهٔ پراکندگی و گسترش ویروس ها در دنیا ابتدا به اینترنت متصل شوید و سپس پنجرهٔ Security Center را در حالت Virus Scan فعال کرده و در پنجرهٔ فوق گزینهٔ View the World ... را کلیک کنید. پس از چند لحظه پنجره ای جهت نمایش نقشهٔ پراکندگی ویروس ها در روی صفحهٔ نمایش ظاهر می شود.

۱

۲

نقشهٔ پراکندگی

راهنمای پراکندگی

۳

٤

۱- از این منو شما می توانید نوع نمایش همهٔ ویروس ها و یا ۱۰ ویروس مطرح دنیا را انتخاب کنید.

۲- از این منو شما می توانید محدودهٔ زمانی پراکندگی ویروس ها را تعیین کنید.

۳- از این منوی کشویی می توانید برای بزرگ و کوچک کردن قسمتی از نقشه استفاده کنید.

۴- از این منوی کشویی شما می توانید منطقهٔ مورد نظرتان را جهت تمرکز روی آن انتخاب کنید.

خلاصهٔ این فصل

ما در این فصل به بررسی قابلیت های مختلف برنامهٔ ضد ویروس McAfee پرداختیم و تجربه های فراوانی در ویروس یابی، تنظیمات و پیکربندی این برنامهٔ جذاب کسب کرده ایم. نگاهی نیز به نحوهٔ فعال سازی برنامهٔ ضد ویروس McAfee و تنظیمات مربوطه داشتیم. نحوهٔ قرنطینه کردن فایل های مشکوک به ویروسی بودن، به روزسازی ضد ویروس و ساخت دیسک نجات را نیز در این فصل گام به گام یکدیگر فرا گرفتیم. به شما تبریک می گوییم حالا ویروس یاب McAfee به عنوان یک برنامهٔ کارآمد در کنار شماست.

فصل ۱۲

معرفی خطرناک‌ترین ویروس‌های دنیا

امسال حدود ٤١ سال از عمر اینترنت می‌گذرد. امروزه اینترنت علی‌رغم جوان بودن نسبت بـه دیگـر رسانه‌ها توانسته است جایگاه ویژه‌ای را در جهان ارتباطات برای خود دست‌و پا کند. بـه طوریکـه حالا تصور نبودن اینترنت بسیار نگران کننده است.

اما علی‌رغم فواید بی‌شمار اینترنت برای انسان امروزی با چالش بزرگی در امنیت اطلاعـات روبـرو است. از همین رو قصد داریم به بررسی خطرناک‌ترین ویروس‌هـا در ۱۰ سـال اخیـر بپـردازیم. آیـا آماده هستید؟

ویروس I Love You

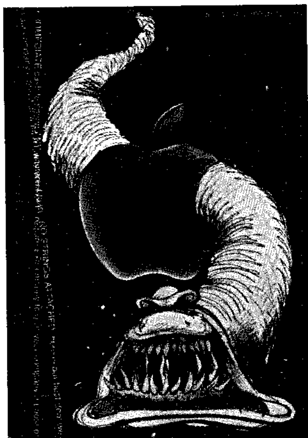
ویروس فوق یکی از خطرناک‌ترین ویروس‌های کامپیوتری بود که تا سـال ۲۰۰۰ توانـست جمعـاً ۵۰ میلیون کامپیوتر را در سراسر دنیا آلوده کند، به نحوی‌که سازمان سیا، پنتـاگون و نهادهـای امنیتـی مهم در انگلستان نیز برای مصون ماندن از خطر این ویروس، خـدمات ایمیـل خـود را موقتـاً از کـار انداختند. جالب اینجاست که در نهایت مشخص شد که نویسندهٔ این ویروس یک فیلیپینی است که پس از دستگیری به دلیل عدم پیش‌بینی قانون در آن کشور تبرئه شد.

I love you

ویروس کانفیر نامیک (کرم اینترنتی)

این کرم اینترنتی روزانه ۵۰ هزار قربانی در سراسر جهان می‌گرفت. روش کار این کرم نیز به این ترتیب بود که اطلاعات محرمانه و شخصی کاربران قربانی را برای طراح این ویروس ارسال می‌کرد. این ویروس آنقدر پیش رفت که غول رایانه‌ای دنیا مایکروسافت برای شناسایی طراحان آن جایزه‌ای ۲۵۰ هزار دلاری در نظر گرفت.

ویروس ملیسا



یکی از ویروس‌های خطرناکی که توجه تمامی رسانه‌های جهان را به خود جلب کرد ملیسا بود. این ویروس پس از ورود به یک سیستم اسناد ایجاد شده توسط برنامهٔ Word را آلوده کرده و باعث بروز برخی تغییرات در تنظیمات سیستم می‌شود. علت توجه به ویروس فوق سرعت بالا و نگران کنندهٔ آن در انتشار و فراگیری آن بود. بطوریکه این ویروس در ظرف ۶ سال همچنان قدرت تخریبی و مهار ناشدنی خود را حفظ کرد و در نهایت تا سال ۲۰۰۵ حدود ۱۵ تا ۲۰ درصد کامپیوترهای کل جهان را آلوده کرد. دیوید اسمیت نویسندهٔ این ویروس بعدها به جرم وارد کردن خساراتی معادل ۸۰ میلیون دلار دستگیر و روانهٔ زندان شد.

ویروس اِسلمر

یکی از ویروس‌هایی که با آلوده‌سازی کامپیوتر، اینترنت را موقتاً از کار انداخت و در نوع خود بی‌نظیر بود، ویروس اسلمر بود. این ویروس ظرف تنها ۱۰ دقیقه نزدیک به ۷۵ هزار قربانی گرفت. موضوعی که بسیاری از کشورها را به این فکر انداخت که با یک حملهٔ تروریستی سازمان یافته و عظیم جهانی به زیر ساخت‌های ارتباطی خود مواجه هستند.

کرم رایانه‌ای کدرد

یکی از ویروس‌های خطرناک اینترنتی **کدرد** نام دارد. این ویروس از نوع کرم اینترنتی بود، که توانست ظرف مدت کوتاهی ۳۵۹ هزار سایت را در دنیا آلوده کند.

ویروس Nimayan

یکی از ویروس‌های خطرناک دنیا در سال ۲۰۰۷ که توانست ظرف مدت ۲ ماه، میلیون‌ها نفر را آلوده کند، ویروس Nimayan نام داشت. این ویروس علاوه بر از بین بردن فایل‌ها از حساب‌های بانکی کاربران نیز سرقت می‌کرد. زادگاه اصلی این ویروس کشور چین است که برخلاف کالاهای نامرغوب چینی دارای عملکرد پرقدرتی بود. نویسندهٔ این ویروس وانگلی نام داشت که در سال ۲۰۰۷ توسط نیروهای امنیتی چین دستگیر شد. وی ادعا می‌کرد، اگر این ویروس تنها چند ماه دیگر عمر می‌کرد می‌توانست تهدیدی جدی علیه رایانه و اقتصاد کشور چین باشد بطوریکه کسی جرأت روشن کردن کامپیوتر خود را نداشته باشد.

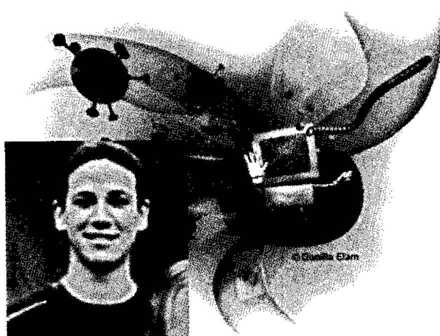
کرم رایانه‌ای موریس و ساسر

یکی از مخرب‌ترین ویروس‌ها در دنیای کامپیوتر ویروس ساسر است. این ویروس به صورت خودکار (پس از نفوذ به سیستم) در رجیستری ویندوز قرار می‌گیرد و با هر بار روشن شدن ویندوز اجرا می‌شود و سعی می‌کند که کامپیوتر را Shutdown کرده و در هربار فعال شدن ویندوز این کار را تکرار می‌کند.

ویروس Netsky

از دیگر ویروس‌های به یاد ماندنی در سال ۲۰۰۴ می‌توان به کردم Netsky اشاره کرد. این ویروس از طریق ایمیل‌های آلوده و با استفاده از مکانیزم SMTP در سطح جهان منتشر شد. این ویروس با جمع‌آوری الکترونیکی از کامپیوترهای قربانی اقدام به ارسال ایمیل‌های آلوده به آنها می‌کند.
این ویروس به محض فعال شدن یک فایل آلوده اجرایی به رجیستری ویندوز اضافه می‌کند. به علاوه ویروس Netsky فایل‌های متعددی را با نام‌های متغیر و پسوند ZIP در درایوهای مختلف ایجاد می‌کند که با اجرای این فایل‌ها پیام دروغینی مبنی بر عدم نمایش فایل فوق ظاهر می‌شود.
نویسنده هر دو ویروس ساسر و Netsky یک جوان ۱۸ ساله آلمانی به نام ون جاخن بود که در سال ۲۰۰۴ دستگیر شد. او در دادگاه مسئول گسترش ۷۰ درصد از کرم‌های رایانه‌ای در آن زمان شناخته شد. البته جاخن پس از آزادی به عنوان مسئول امنیت شبکه در یک شرکت بزرگ امنیت اطلاعات استخدام شد.





کرم رایانه‌ای Storm

این کرم با عنوان خبر فوری: «هوای بد و طوفانی کل اروپا را در نوردیده است» توانست در اندک زمانی میلیون‌ها کامپیوتر را در سراسر دنیا آلوده کند. این ویروس از نوع تروجان بوده و پس از باز شدن تمامی سیستم رایانه‌ای را آلوده می‌کند. این ویروس Storm با ایجاد یک حفرهٔ امنیتی در سیستم آنها را در مقابل هکرها و ویروس‌های کامپیوتری آسیب‌پذیر می‌کند. این ویروس دارای گونه‌های متعددی است.

ویروس چرنویل

ویروس چرنویل یا به اختصار CIH هر سال در ۲۶ آوریل (۶ اردیبهشت) همزمان با سالگرد فاجعهٔ هسته‌ای چرنوبیل فعال می‌شود. تا به حال خسارات فراوانی را به کامپیوترهای سراسر دنیا وارد کرده است. این ویروس با وارد کردن اطلاعاتی در یکی از تراشه‌های اصلی کامپیوتر می‌تواند باعث از کار افتادن آن شود. نویسندهٔ این ویروس یک تایوانی به نام چن ایگ هو بود که توسط پلیس تایوان دستگیر شد.

کرم رایانه‌ای Blaster

از خطرناک‌ترین ویروس‌های سال ۲۰۰۳ می‌توان به کرم رایانه‌ای Blaster اشاره کرد که با استفاده از حفرهٔ امنیتی موجود در ویندوز XP مایکروسافت میلیون‌ها کامپیوتر را در سراسر دنیا آلوده کرد. این ویروس پس از ورود به یک سیستم هنگام اتصال به اینترنت بعد از ۶۰ ثانیه کامپیوتر را خاموش می‌کند. نسخه‌های مختلفی از این ویروس هر روز در حال تولید است.



ویروس My Doom

یکی از ویروس‌های خطرناک که به سرعت در سراسر جهان گسترش پیدا کرد، ویروس My Doom است. گستردگی این ویروس به حدی بود که مایکروسافت جایزه‌ای ۲۵۰ هزار دلاری برای معرفی نویسنده این ویروس خطرناک در نظر گرفت.
ویروس فوق به صورت یک فایل پیوستی توسط ایمیل و به صورت تصادفی ارسال می‌شود. ویروس فوق به محض اجرا شدن توسط یک گیرندهٔ از همه جا بی‌خبر یک کپی از کد اصلی ویروس را در دایرکتوری سیستم و رجیستری باعث اجرای سیستم با هر بار فعال شدن کامپیوتر می‌شود. این ویروس کارکرد اصلی سیستم را مختل کرده و ترافیک شبکه اینترنت را تا حد زیادی بالا می‌برد. نسخه‌های جدید ویروس My Doom توسط ایمیل‌های حاوی تصاویر مستهجن شروع به انتشار می‌کند و به محض ورود نرم‌افزار امنیتی کامپیوتر را از کار انداخته و کامپیوتر را تبدیل به یک زامبی می‌کند.

ویروس Conficker

این ویروس در سال ۲۰۰۸ منتشر شده و تا کنون دست کم ۱۰ میلیون کامپیوتر را در سراسر دنیا آلوده کرده است. این ویروس تنها کامپیوترهایی را آلوده می‌کند که از سیستم عامل ویندوز استفاده می‌کنند. این ویروس برای نفوذ از یک حفرهٔ امنیتی ویندوز به نام MS08-67 استفاده می‌کند. این ویروس دقیقاً در روز تحلیف رئیس‌جمهور آمریکا باراک اوباما منتشر شد و ادعا می‌کند که اوباما به صورت ناگهانی از سمت رئیس جمهوری کنار گرفته است و از کاربر می‌خواهد برای مشاهدهٔ این خبر بر روی یک لینک اینترنتی کلیک کند. تغییر رجیستری سیستم عامل و ایجاد حفره‌های متعدد امنیتی در شبکه‌های رایانه‌ای از جمله عملکردهای مخرب این کرم محسوب می‌شود.

کرم Sobig

یکی از ویروس‌های خطرناک در سال ۲۰۰۲ که باعث از کار افتادن کامپیوترهای وزارت دفاع آمریکا و هواپیمایی کانادا شد کرم Sobig است. این ویروس از سیستم‌های آلوده به عنوان یک مولد Spam و زامبی استفاده کرده و توانایی انهدام شبکه‌های محلی را در هر نوع ساختار دارد.

ویروس ویکی‌لیکس

این ویروس که به صورت هوشمندانه از مشهور بودن سایت ویکی‌لیکس سوء استفاده کرده و در اواخر سال ۲۰۱۰ توانست کامپیوترهای زیادی را در دنیا آلوده کند. این ویروس در یک فایل PDF جاخوش کرده و از طریق ایمیل گسترش می‌یابد. هدف اصلی این ویروس دستیابی به اطلاعات کاربر و رمز عبور وی است.

ویروس استاکس نت

یکی از ویروس‌های بسیار پیشرفته‌ای که در سال ۲۰۱۰ سر و صدای زیادی به پا کرد ویروس استاکس نت است. این ویروس اولین بار در اوایل مرداد ماه توسط یک شرکت کوچک امنیتی در بلاروس گزارش شد.

این ویروس توسط متخصصان رژیم اشغالگر قدس و با هدف ضربه زدن به تحقیقات هسته‌ای ایران ایجاد گردیده است. متأسفانه این ویروس بیشترین قربانی‌های خود را از ایران گرفته است. ایجاد و انتشار این ویروس را می‌توان یک جنگ سایبری بر علیه کشور عزیزمان دانست.

آیا استاکس نت یک اَبَر ویروس است؟

شاید در نگاه اول، کرم رایانه ای "استاکس نت"، یکی از مخرب ترین و کوبنده ترین بدافزارهایی باشد که پهنه اینترنت را درنوردیده اند و در زیرکانه ترین و موذیانه ترین وضعیت ممکن به درون شبکه‌های سازمانی نفوذ کرده اند. اما این ویروس چموش، هرگز یک نمونه بزرگ از کدهای مخرب بسیار خطرناک نظیر Slammer، I Love You، Conficker و Sality محسوب نمی‌شود، حتی اگر به مدد رسانه ها و مراکز خبری قدرتمند و یا محافل سیاسی جهان، نام آن بر سرزبان ها افتاده باشد.

در یک کلام، استاکس نت بیش از آنکه از لحاظ فنی بزرگ و خطرناک باشد، از لحاظ رسانه ای و سیاسی به یک اَبَرویروس مخرب تبدیل شده است. دلایل بسیاری برای این ادعا وجود دارد که با مطالعه رفتار و نحوه عملکرد این کرم رایانه ای، کاملاً قانع کننده به نظر می رسند.

سنگی بزرگ برای " نزدن "!

تحلیل‌های بیشتر بر روی نحوه کدنویسی و رفتار استاکس نت نشان میْ دهد که این کرم رایانه ای، یک بدافزار کاملاً مهاجم و خطرناک است که با هدف سرقت اطلاعات حساس و ایجاد اختلال در فرایندهای حیاتی مراکز استراتژیک، منتشر شده است. تمام شرکت‌های امنیتی روی این موضوع اتفاق نظر دارند که در صورت مهیا بودن شرایط مناسب، این کرم می تواند حتی زیرساخت‌های حیاتی یک کشور را نیز به خطر بیاندازد. اما نکته ظریفی که هیچ گاه و در هیچ تحلیلی مورد توجه



کافی قرار نگرفت این است که شرایط لازم و کافی برای انتشار و حمله یک ویروس رایانه ای، هر چند مهاجم و زیرک، به مراکز حساس و استراتژیک یک کشور، تا چه حد امکان تحقق دارند؟
یا اصولاً یک ویروس بسیار مخرب مانند Stuxnet، از چه طریقی می تواند به "رایانه‌های هدف" نفوذ کند و پس از آن تا چه مقدار موفق به پی گیری فعالیت‌های تخریبی خود خواهد شد؟
و آیا تدابیر، سیاست ها و راهکارهای حفاظتی بکارگرفته شده در حیاتی ترین زیر ساخت‌های یک کشور، امکان نفوذ یک ویروس رایانه ای هر چند بسیار خطرناک را فراهم می آورد؟
واقعیت این است که استاکس نت با تمام قابلیت‌های تخریبی و خطرناک خود، به یک سنگ بزرگ شبیه است که قابل پرتاب به سمت هدف خود نیست.

آیا استاکس نت به اهداف خود رسید؟

استاکس نت، درست مانند سایر ویروس ها و کدهای مخرب، بی نیاز از ابزار و روش‌های ارتباطی برای نفوذ به رایانه ها و سیستم‌های نیست. اتصال به اینترنت، استفاده از حافظه‌های جانبی نامطمئن، وجود شبکه‌های داخلی و منابع اشتراک فایل و ... از شرطهای لازم برای انتشار استاکس نت و سپس نفوذ به سیستم‌های هدف محسوب می شود. بنابر این یکی از بهترین راه‌های ایمن کردن یک سیستم فوق محرمانه که حاوی اطلاعات استراتژیک یا تنظیمات حساس عملیاتی ست، اطمینان از مسدود بودن کلیه راه‌های نفوذ اطلاعات، حذف ارتباط و منابع اشتراک فایل با سایر رایانه‌ها و استفاده بسیار محدود از حافظه‌های جانبی می باشد. به نظر می رسد که این موارد، حداقل شروط امنیتی ست که در مراکز کلان اداری و صنعتی یک کشور و برای سیستم ها و رایانه‌های بسیار حساس اعمال می شود. خنده دار است اگر تصور کنیم که در تأسیسات حیاتی یک شرکت یا سازمان بزرگ، کلیه راه‌های نفوذ یک ویروس بررسی و مسدود نشده باشند. به این ترتیب و با این فرض اثبات شده که هدف استاکس نت رایانه‌های حساس سازمانی و تجهیزات کنترل پروژه‌های زیرساخت مانند سیستم‌های SCADA با حداکثر مراقبت‌های امنیتی بوده است، به نظر نمی رسد که این کرم رایانه ای، شرایط خیلی مناسبی برای رسیدن به نقاط هدف داشته و "در عمل" تهدید چندانی برای مراکز استراتژیک کشورها بوده باشد.

آمارهای نامطمئن!

علاوه بر این، آمارهایی که انتشار و میزان پراکندگی استاکس نت را ثبت کرده اند، تضمینی برای نفوذ و عملکرد موفق این ویروس در رایانه‌های هدف (شبکه‌های زیرساخت و حیاتی یک کشور) نیستند. چرا که اگر فایل مخرب استاکس نت، در یک رایانه خانگی و توسط یک ضدویروس خاص کشف شده باشد، گزارش آلودگی "ناموفق" این کرم در یک "رایانه غیر هدف"، به آمار کلی منتشر شده اضافه می گردد. با توجه به این مسئله که هر شرکت امنیتی به طور انحصاری، یک سیستم

آماری مستقل را در اختیار دارد، باید دید که برای مثال حفاظت چند درصد از رایانه ها و شبکه‌های سازمانی یک کشور به عهده آن شرکت خاص ست تا بتوان با استناد به آمارهای منتشر شده، متوسطی از میزان شیوع ویروس را در کل کشور بدست آورد. البته تا کنون هیچ مرجع عمومی و بین المللی نتوانسته، با همکاری شرکت‌های امنیتی مهم، یک آمار جامع از میزان انتشار استاکس نت منتشر کند.

چگونه در برابر استاکس نت یا گونه‌های پیشرفته تر آن، ایمن بمانیم؟

شواهد و قرائن موجود، نشان می دهند که استاکس نت به هیچ عنوان یک تهدید "عملی" علیه شبکه زیرساخت هیچ کشوری نبوده است؛ هر چند بلوف‌های سیاسی و فرضیه‌های تخریبی بسیاری برای آن مطرح شده است. البته می توان این کرم رایانه ای را به عنوان یک نمونه پیشرو و خلاق از ویروس‌های پیشرفته تری در نظر گرفت که در صورت عدم توجه کافی مدیران شبکه‌های سازمانی، عامل ایجاد خسارت‌های غیرقابل جبران باشند. به بیان دیگر استاکس نت هر چند در عمل تخریب چندانی به بار نیاورده، اما تجربه لذت بخشی برای خرابکاران و تبهکاران اینترنتی بوده است تا به این کرم، به عنوان یک مدل مناسب برای طرح ریزی حملات آینده خود نگاه کنند.

باید اعتراف کرد که **"یک رایانه امن، یک رایانه خاموش است"** و یا دست کم رایانه‌ای است که ارتباطات ورودی یا خروجی آن مسدود یا به شدت تحت حفاظت باشد. بنابراین رایانه‌ها و شبکه‌هایی که ناگزیر از اتصال به اینترنت یا شبکه‌های داخلی هستند، باید از تمامی روش‌های امنیتی ممکن برای حفاظت از اطلاعات و تجهیزات خود بهره بگیرند.

پشتیبانی محلی یا آنلاین اطلاعات بسیار حساس، رمزگذاری داده‌های محرمانه، استفاده از نرم‌افزارهای امنیتی مجهز به روش‌های پیشگیرانه ضدویروس، بروزرسانی سیستم‌های عامل و برنامه‌های کاربردی مهم و ... می توانند کاربران خانگی را در حفاظت مؤثر از اطلاعات ارزشمند و محرمانه یاری کنند.

برای شبکه‌های سازمانی کوچک، متوسط و بزرگ نیز، "سخت افزارهای امنیتی" بهترین گزینه برای پیشگیری از ورود تهدیدهایی مانند استاکس نت به درون محیط عملیاتی سازمان محسوب می شوند. این دستگاه ها در نقطه اتصال شبکه به اینترنت قرار می گیرند و با شناسایی هر نوع فایل اجرایی با رفتار مخرب و حرکت مشکوک، از نفوذ آن به درون شبکه جلوگیری کرده و تهدیدهای ورودی از اینترنت را در بیرون از محیط عملیاتی سازمان، کشف و خنثی می کنند.

این ابزار و راهکارهای امنیتی باید جدی گرفته شوند، زیرا استاکس نت، فقط پیش قراول جنگ‌های رایانه ای آینده است که می توانند زیرساخت‌های حیاتی کشورها را به صورت "عملی" تهدید کنند.